BY EXPRESS MAIL NO. EL776051240US
Attorney Docket No. KOIK-T0343

WO 00/58827
PCT/JP00/02041

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:
KOIKE, Akira
No.11 Mori Building
6-4, Toranomon 2-chome
Minato-ku
Tokyo 105-0001
JAPON

Date of mailing (day/month/year) 05 October 2000 (05.10.00)	
Applicant's or agent's file reference SK00PCT31	**IMPORTANT NOTICE**

International application No.	**International filing date** (day/month/year)	**Priority date** (day/month/year)
PCT/JP00/02041	30 March 2000 (30.03.00)	30 March 1999 (30.03.99)

Applicant
SONY CORPORATION et al

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
   AG,AU,DZ,KP,KR,US

   In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
   AE,AL,AM,AP,AT,AZ,BA,BB,BG,BR,BY,CA,CH,CN,CR,CU,CZ,DE,DK,DM,EA,EE,EP,ES,FI,GB,GD,
   GE,GH,GM,HR,HU,ID,IL,IN,IS,KE,KG,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,NO,
   NZ,OA,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW
   The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
   05 October 2000 (05.10.00) under No. WO 00/58827

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, **a demand for international preliminary examination** must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the **national phase**, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer J. Zahra
Facsimile No. (41-22) 740.14.35	Telephone No. (41-22) 338.83.38

Form PCT/IB/308 (July 1996)

3550998

BY EXPRESS MAIL NO. EL776051240US
Attorney Docket No. KOIK-T0343

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/02041

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-5 relate to an information providing apparatus for receiving a program from a program information processing device over a network, encrypting the received program, and transmitting it to information processing device, to an information providing method, and to a program providing medium.

There is no special technical feature common to the inventions of claims 6-52 and those of claims 1-5.

For example, the inventions of claims 6-8 relate to an information processing apparatus for selecting a mutual authentication to be made from among mutual authentications between information processing devices and carrying out the mutual authentication, to an information processing method, and to a program providing medium.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/02041

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F 1/00, 3/06, 3/08, 9/06, 9/445, 12/14, 13/00, 17/60
H04L 9/00-9/32
G09C 1/00-5/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DIALOG(INSPEC): OpenMG, MagicGate, MemoryStick
JICST(JOIST) : OpenMG, MagicGate, MemoryStick, Copyright, Contents Down Load

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Taro Yoshio, "Digital Chosakuken:Kogata Memory Card de Chosakuken wo mamoru", *Nikkei Electronics*, No.739, 22 March, 1999 (Tokyo), p.49-53	1-52
X Y	Taro Yoshio, "Ongaku Haishin matta nashi: Seibi Isogu Chosakuken Hogo Gijutsu", *Nikkei Electronics*, No.738, 08 March, 1999 (Tokyo), p.94-98	11-14 1-10,15-52
Y	EP, 875815, A2 (SONY CORPORATION), 04 November, 1998 (04.11.98), Full text; Figs. 1 to 16 & JP, 10-301772, A	1-5,15-52
Y	EP, 875814, A2 (SONY CORPORATION), 04 November, 1998 (04.11.98), Full text; Figs. 1 to 22 & JP, 10-301773, A	1-5,15-52
Y	EP, 862293, A2 (MATSUSHITA ELECTRIC INDUSTRIAL CO.LTD.), 02 September, 1998 (02.09.98), Full text; Figs. 1 to 9 & JP, 10-304333, A	6-8

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 June, 2000 (21.06.00)	04 July, 2000 (04.07.00)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/02041

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"DVD, Personal Computer ni noru Software Fukugou no Kagi wo nigiru Fusei Copy Boushi Gijutsu no Medo", *Nikkei Electronics*, No.696, 18 August, 1997 (Tokyo), p.110-119	9-10,15-52
Y	David Aucsmith, "Gyaku Kaiseki ya Kaihen kara Soft wo mamoru Tamper Resistant Software Gijutsu no Shousai", *Nikkei Electronics*, No.706, 05 January, 1998 (Tokyo), p.209-220	9-10,15-52
Y	EP, 874299, A2 (SONY CORPORATION), 28 October, 1998 (28.10.98), Full text; Figs. 1 to 32 & JP, 11-53264, A	9-10
Y	EP, 874300, A2 (SONY CORPORATION), 28 October, 1998 (28.10.98), Full text; Figs. 1 to 41 & JP, 11-53264, A	9-10
A	WO, 96/27155, A1 (INTERTRUST TECHNOLOGIES CORP.), 06 September, 1996 (06.09.96), Full text; Figs. 1 to 87 & JP, 10-512074, A	1-52

EP・US

特　許　協　力　条　約

PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人 の書類記号　SK00PCT31	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０２０４１	国際出願日 （日.月.年）　３０．０３．００	優先日 （日.月.年）　３０．０３．９９
出願人（氏名又は名称） ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　4　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ｉ欄参照）。

３．☒ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　2　図とする。☒ 出願人が示したとおりである。　／☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際[redacted]報告

国際出[redacted]号　PCT／JP00／02041

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１－５はネットワークを介してプログラムを情報処理装置からプログラムを受信し、受信したプログラムを暗号化して、前記情報処理装置に送信する構成を有する情報提供装置、情報提供方法およびプログラム提供媒体に関するものである。

一方、請求項６－５２については上記の構成とは共通の特別な技術的特徴はない。

たとえば、請求の範囲６－８は情報処理装置間の相互認証を行う際において、１以上の相互認証の手続きから、実行する相互認証の処理を選択し、実行する構成を有する情報処理装置、情報処理方法およびプログラム提供媒体に関するものである。

1．☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

国際[redacted]報告

国際出[redacted]号 PCT／JP00／02041

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））
Ｉｎｔ Ｃｌ' Ｇ06Ｆ9／06

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Ｉｎｔ Ｃｌ' Ｇ06Ｆ 1/00, 3/06, 3/08, 9/06, 9/445, 12/14, 13/00, 17/60
Ｈ04Ｌ 9／00～9／32
Ｇ09Ｃ 1／00～5／00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報 １９２２－１９９６年
日本国公開実用新案公報 １９７１－２０００年
日本国登録実用新案公報 １９９４－２０００年
日本国実用新案登録公報 １９９６－２０００年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
DIALOG(INSPEC): OpenMG, MagicGate, MemoryStick
JICST(JOIST) : OpenMG, MagicGate, メモリースティック, 著作権, コンテンツ配信

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y ✓	日経エレクトロニクス, 第739号, 22. 3月. 1999(東京), 芳尾太郎, "ディジタル著作権：小型メモリ・カードで著作権を守る", p. 49-53	1-52
X ✓ Y	日経エレクトロニクス, 第738号, 08. 3月. 1999(東京), 芳尾太郎, "音楽配信待ったなし・整備急ぐ著作権保護技術", p. 94-98	11-14 1-10, 15-52
Y ✓	EP, 875815, A2(SONY CORPORATION) 4. 11月. 1998(04. 11. 98) 全文, 第１～１６図 &JP, 10-301772, A	1-5, 15-52

☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 ２１．０６．００	国際調査報告の発送日 04.07.00
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 田川 泰宏 ５Ｂ ４２３６ 電話番号 ０３－３５８１－１１０１ 内線 ３５４５

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	EP, 875814, A2 (SONY CORPORATION) 4.11月.1998 (04.11.98) 全文, 第１～２２図 &JP, 10-301773, A	1-5, 15-52
Y	EP, 862293, A2 (MATSUSHITA ELECTRIC INDUSTRIAL CO.LTD.) 2.9月.1998 (02.09.98) 全文, 第１～９図 &JP, 10-304333, A	6-8
Y	日経エレクトロニクス, 第696号, 18.8月.1997 (東京), "ＤＶＤ、パソコンに載る　ソフトウェア復号のカギを握る不正コピー防止技術のメド", p.110-119	9-10, 15-52
Y	日経エレクトロニクス, 第706号, 05.1月.1998 (東京), David Aucsmith, "逆解析や改変からソフトを守る タンパ・レジスタント・ソフトウエア技術の詳細", p.209-220	9-10, 15-52
Y	EP, 874299, A2 (SONY CORPORATION) 28.10月.1998 (28.10.98) 全文, 第１～３２図 &JP, 11-53264, A	9-10
Y	EP, 874300, A2 (SONY CORPORATION) 28.10月.1998 (28.10.98) 全文, 第１～４１図 &JP, 11-53264, A	9-10
A	WO, 96/27155, A1 (INTERTRUST TECHNOLOGIES CORP.) 6.9月.1996 (06.09.96)　全文, 第１～８７図 &JP, 10-512074, A	1-52

THIS PAGE BLANK (USPTO)

国際[redacted]報告

国際出[redacted]号 PCT／JP00／00932

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. cl⁷ C02F 3／10, 3／28, 3／06, C12N 11／00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. cl⁷ C02F 3／10, 3／28, 3／06, C12N 11／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案広報	1926－1996
日本国公開実用新案広報	1971－2000
日本国登録実用新案広報	1994－2000
日本国実用新案登録広報	1996－2000

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

WPI（DIALOG） C02F-003*magnetic

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP, 11－18765, A（科学技術振興事業団） 26. 1月. 1999（26. 01. 99）, ファミリーなし	1-3, 5, 7, 10-16
Y	請求項1－3, 【0027】－【0039】, 図1－7	4, 6, 9, 17
A		8
Y	JP, 3－254895, A（株式会社西原環境衛生研究所） 13. 11月. 1991（13. 11. 91）, ファミリーなし 第2頁右下欄第9－15行	4, 6
Y	JP, 8－257589, A（日本碍子株式会社）	4, 6, 17

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 23. 05. 00	国際調査報告の発送日 30.05.00
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 吉水 純子 印 4D 7738 電話番号 03－3581－1101 内線 6425

様式PCT／ISA／210（第2ページ）（1998年7月）

特許協力条約に基づく国際出願願書 SK00PCT31
副本 - 印刷日時 2000年03月30日 (30.03.2000) 木曜日 14時36分01秒

0	受理官庁記入欄	
0-1	国際出願番号.	
0-2	国際出願日	
0-3	(受付印)	

PCT
30.3.'00
受領印

0-4	様式-PCT/RO/101 この特許協力条約に基づく国際出願願書は、	
0-4-1	右記によって作成された。	PCT-EASY Version 2.90 (updated 08.03.2000)
0-5	申立て 出願人は、この国際出願が特許協力条約に従って処理されることを請求する。	
0-6	出願人によって指定された受理官庁	日本国特許庁 (RO/JP)
0-7	出願人又は代理人の書類記号	SK00PCT31
I	発明の名称	情報処理システム
II	出願人	
II-1	この欄に記載した者は	出願人である (applicant only)
II-2	右の指定国についての出願人である。	米国を除くすべての指定国 (all designated States except US)
II-4ja	名称	ソニー株式会社
II-4en	Name	SONY CORPORATION
II-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号
II-5en	Address:	7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
II-6	国籍 (国名)	日本国 JP
II-7	住所 (国名)	日本国 JP
III-1	その他の出願人又は発明者	
III-1-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-1-2	右の指定国についての出願人である。	米国のみ (US only)
III-1-4ja	氏名(姓名)	石黒 隆二
III-1-4en	Name (LAST, First)	ISHIGURO, Ryuji
III-1-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-1-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-1-6	国籍 (国名)	日本国 JP
III-1-7	住所 (国名)	日本国 JP

特許協力条約に基づく国際出願願書 SK00PCT31
副本 - 印刷日時 2000年03月30日 (30.03.2000) 木曜日 14時36分01秒

III-2	その他の出願人又は発明者	
III-2-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-2-2	右の指定国についての出願人である。	米国のみ (US only)
III-2-4ja	氏名(姓名)	河上 達
III-2-4en	Name (LAST, First)	KAWAKAMI, Itaru
III-2-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-2-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-2-6	国籍 (国名)	日本国 JP
III-2-7	住所 (国名)	日本国 JP
III-3	その他の出願人又は発明者	
III-3-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-3-2	右の指定国についての出願人である。	米国のみ (US only)
III-3-4ja	氏名(姓名)	田辺 充
III-3-4en	Name (LAST, First)	TANABE, Mitsuru
III-3-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-3-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-3-6	国籍 (国名)	日本国 JP
III-3-7	住所 (国名)	日本国 JP
III-4	その他の出願人又は発明者	
III-4-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-4-2	右の指定国についての出願人である。	米国のみ (US only)
III-4-4ja	氏名(姓名)	江面 裕一
III-4-4en	Name (LAST, First)	EZURA, Yuichi
III-4-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-4-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-4-6	国籍 (国名)	日本国 JP
III-4-7	住所 (国名)	日本国 JP

特許協力条約に基づく国際出願願書 SK00PCT31
副本 - 印刷日時 2000年03月30日 (30.03.2000) 木曜日 14時36分01秒

III-5	その他の出願人又は発明者	
III-5-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-5-2	右の指定国についての出願人である。	米国のみ (US only)
III-5-4ja	氏名(姓名)	河原 博和
III-5-4en	Name (LAST, First)	KAWAHARA, Hirokazu
III-5-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-5-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-5-6	国籍 (国名)	日本国 JP
III-5-7	住所 (国名)	日本国 JP
IV-1	代理人又は共通の代表者、通知のあて名 下記の者は国際機関において右記のごとく出願人のために行動する。	代理人 (agent)
IV-1-1ja	氏名(姓名)	小池 晃
IV-1-1en	Name (LAST, First)	KOIKE, Akira
IV-1-2ja	あて名:	105-0001 日本国 東京都 港区 虎ノ門二丁目６番４号 第１１森ビル
IV-1-2en	Address:	No.11 Mori Bldg., 6-4, Toranomon 2-chome Minato-ku, Tokyo 105-0001 Japan
IV-1-3	電話番号	03-3508-8266
IV-1-4	ファクシミリ番号	03-3508-0439
IV-2	その他の代理人	筆頭代理人と同じあて名を有する代理人 (additional agent(s) with same address as first named agent)
IV-2-1ja	氏名	田村 榮一; 伊賀 誠司
IV-2-1en	Name(s)	TAMURA, Eiichi; IGA, Seiji
V	国の指定	
V-1	広域特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	AP: GH GM KE LS MW SD SL SZ TZ UG ZW 及びハラレプロトコルと特許協力条約の締約国である他の国 EA: AM AZ BY KG KZ MD RU TJ TM 及びユーラシア特許条約と特許協力条約の締約国である他の国 EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE 及びヨーロッパ特許条約と特許協力条約の締約国である他の国 OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG 及びアフリカ知的所有権機構と特許協力条約の締約国である他の国

特許協力条約に基づく国際出願願書 SK00PCT31
副本 - 印刷日時 2000年03月30日 (30.03.2000) 木曜日 14時36分01秒

V-2	国内特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	AE AG AL AM AT AU AZ BA BB BG BR BY CA CH&LI CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW	
V-5	指定の確認の宣言 出願人は、上記の指定に加えて、規則4.9(b)の規定に基づき、特許協力条約のもとで認められる他の全ての国の指定を行う。ただし、V-6欄に示した国の指定を除く。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。		
V-6	指定の確認から除かれる国	なし (NONE)	
VI-1	先の国内出願に基づく優先権主張		
VI-1-1	先の出願日	1999年03月30日 (30.03.1999)	
VI-1-2	先の出願番号	平成11年特許願第088346号	
VI-1-3	国名	日本国 JP	
VII-1	特定された国際調査機関(ISA)	日本国特許庁 (ISA/JP)	
VIII	照合欄	用紙の枚数	添付された電子データ
VIII-1	願書	5	-
VIII-2	明細書	117	-
VIII-3	請求の範囲	19	-
VIII-4	要約	1	absk00pct31.txt
VIII-5	図面	48	-
VIII-7	合計	190	
	添付書類	添付	添付された電子データ
VIII-8	手数料計算用紙	✓	-
VIII-9	別個の記名押印された委任状	✓	-
VIII-12	優先権証明書	優先権証明書 VI-1	-
VIII-16	PCT-EASYディスク	-	フレキシブルディスク
VIII-17	その他	納付する手数料に相当する特許印紙を貼付した書面	-
VIII-18	要約書とともに提示する図の番号	2	
VIII-19	国際出願の使用言語名:	日本語 (Japanese)	
IX	提出者の記名押印		
IX-1	氏名(姓名)		
IX-2	権限		

特許協力条約に基づく国際出願願書 SK00PCT31

副本 - 印刷日時 2000年03月30日 (30.03.2000) 木曜日 14時36分01秒

受理官庁記入欄

10-1	国際出願として提出された書類の実際の受理の日	
10-2 10-2-1 10-2-2	図面 : 受理された 不足図面がある	
10-3	国際出願として提出された書類を補完する書類又は図面であってその後期間内に提出されたものの実際の受理の日 (訂正日)	
10-4	特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP
10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	

国際事務局記入欄

11-1	記録原本の受理の日	

世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類7 G06F 9/06	A1	(11) 国際公開番号	WO00/58827
		(43) 国際公開日	2000年10月5日(05.10.00)

(21) 国際出願番号 PCT/JP00/02041

(22) 国際出願日 2000年3月30日(30.03.00)

(30) 優先権データ
特願平11/88346 1999年3月30日(30.03.99) JP

(71) 出願人（米国を除くすべての指定国について）
ソニー株式会社(SONY CORPORATION)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
石黒隆二(ISHIGURO, Ryuji)[JP/JP]
河上 達(KAWAKAMI, Itaru)[JP/JP]
田辺 充(TANABE, Mitsuru)[JP/JP]
江面裕一(EZURA, Yuichi)[JP/JP]
河原博和(KAWAHARA, Hirokazu)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号
ソニー株式会社内 Tokyo, (JP)
(74) 代理人
小池 晃, 外(KOIKE, Akira et al.)
〒105-0001 東京都港区虎ノ門二丁目6番4号
第11森ビル Tokyo, (JP)

(81) 指定国 AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), ARIPO特許 (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM)

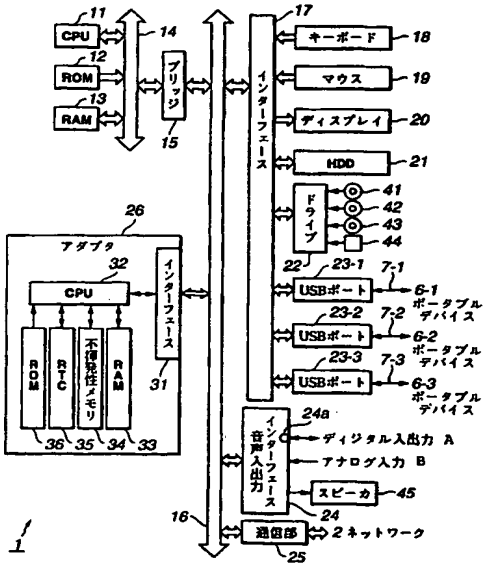
添付公開書類
国際調査報告書

(54)Title: INFORMATION PROCESSING SYSTEM

(54)発明の名称 情報処理システム

(57) Abstract

A personal computer (1) transmits a source program to which a signature is attached to an authenticating station through a communication unit (25). The authenticating station, if no alteration is found in the received source program, encrypts the source program with a secret key of the authenticating station, and transmits the encrypted source program to the personal computer (1). The personal computer (1) records the encrypted source program on an HDD (21) and transmits it to an adapter (26).



24a...INTERFACE AUDIO INPUT/OUTPUT
A...DIGITAL INPUT/OUTPUT
B...ANALOG INPUT
45...LOUDSPEAKER
25...COMMUNICATION UNIT
2...NETWORK
15...BRIDGE
26...ADAPTER
31...INTERFACE
34...NONVOLATILE MEMORY
17...KEYBOARD
18...INTERFACE
19...MOUSE
20...DISPLAY
22...DRIVE
23-1...USB PORT
23-2...USB PORT
23-3...USB PORT
6-1...PORTABLE DEVICE
6-2...PORTABLE DEVICE
6-3...PORTABLE DEVICE

(57)要約

パーソナルコンピュータ１は、通信部２５を介して、認証局に署名を付したソースプログラムを送信し、認証局は、受信したソースプログラムに改竄が発見さなかった場合、受信したソースプログラムを認証局の秘密鍵で暗号化してパーソナルコンピュータ１に送信する。パーソナルコンピュータ１は、認証局から受信した暗号化されたソースプログラムをＨＤＤ２１に記録するとともにアダプタ２６に送信する。

明細書

情報処理システム

技術分野

本発明は、情報提供装置、情報処理方法及び認証方法、半導体ＩＣ、情報処理システム、並びにプログラム提供媒体に関し、特に、所定のデータを記憶し、所定の処理を行うための情報処理装置、情報処理方法及び認証方法、半導体ＩＣ、情報処理システム、並びにプログラム提供媒体に関する。

背景技術

最近、ＣＤ(Compact Disk)、ＭＤ(Mini Disk) といった音楽データをデジタル的に記録又は再生することができる装置が普及してきた。その結果、このようなデジタル的に音楽データを記録再生できる装置をパーソナルコンピュータなどと組み合わせることで、デジタル音楽データを不正に複製することも比較的容易に行うことができるようになってきた。そこで、著作物としての音楽データを不正に複製することができないようにするために、各種の方法が提案されている。

例えば、コピー元を制御するソフトウエアに、コピー先の装置と相互認証させ、適正な認証結果が得られたとき、音楽データを暗号化して、コピー先の装置に転送させ、コピー先の装置において、その暗号化されたデータを復号して利用するようにすることが提案されている。

また、コピー元のソフトウエアに所定のハードウエアに記憶されている識別情報ＩＤを利用して、コピー先の装置と相互認証させることも提案されている。

さらにまた、認証、暗号及び復号処理を、ワイアードロジックのハードウエアで実行させることも提案されている。

しかしながら、ソフトウエアだけで認証処理、暗号化処理及び復号処理を行うようにする場合、ソフトウエアを解析し、改竄することで、音楽データが不正に複製されてしまう恐れがある。

また、所定のＩＤをハードウエアに記憶させ、パーソナルコンピュータ上のソフトウエアにより、これを読み出し、利用させるようにする場合、読み出されたＩＤがソフトウエアに転送される途中において読み取られ、解析、改竄されてしまう恐れがあった。

さらに、認証処理、暗号化処理及び復号処理をワイアードロジックのハードウエアにより実行するようにすると、解析や改竄は防止することが可能であるが、新たな認証処理、暗号化処理及び復号処理を行うようにするには、既存のハードウエアを新たなハードウエアと交換するか、新たなハードウエアを追加する必要が生じる。

発明の開示

本発明は、このような状況に鑑みてなされたものであり、記憶されているデータが不正に読み出され、解析されることを防止できるようにするものである。

すなわち、本発明は、ネットワークを介して、所定の情報処理装置に接続されている情報提供装置において、前記情報処理装置から所定のプログラムを受信するとともに、暗号化された前記プログラムを前記情報処理装置に送信する通信手段と、通信手段が受信した前記プログラムを暗号化する暗号化手段とを含むことを特徴とする。

また、本発明は、ネットワークを介して、所定の情報処理装置に接続されている情報提供装置の情報提供方法において、前記情報処理装置から所定のプログラムを受信するとともに、暗号化された前記プログラムを前記情報処理装置に送信する通信ステップと、通信ステップで受信した前記プログラムを暗号化する暗号化ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、ネットワークを介して、所定の情報処理装置に接続されている情報提供装置に、前記情報処理装置から所定のプログラムを受信するとともに、暗号化された前記プログラムを前記情報処理装置に送信する通信ステップと、通信ステップで受信した前記プログラムを暗号化する暗号化ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、他の情報処理装置と相互認証して、所定の処理を実行する情報処理装置において、前記所定の処理に対応し、１以上の相互認証の手続から、実行する相互認証の処理を選択する選択

手段と、前記選択手段が選択された相互認証の手続を実行する相互認証手段とを含むことを特徴とする。

また、本発明は、他の情報処理装置と相互認証して、所定の処理を実行する情報処理装置の情報処理方法において、前記所定の処理に対応し、１以上の相互認証の手続から、実行する相互認証の処理を選択する選択ステップと、前記選択ステップで選択された相互認証の手続を実行する相互認証ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、他の情報処理装置と相互認証して、所定の処理を実行する情報処理装置に、前記所定の処理に対応し、１以上の相互認証の手続から、実行する相互認証の処理を選択する選択ステップと、前記選択ステップで選択された相互認証の手続を実行する相互認証ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明に係る認証方法は、第１装置において第１乱数を発生し、第１装置の識別情報と鍵の属性情報と上記第１乱数とを第１装置から第２装置に送信し、第２装置において第２乱数を発生し、第２装置において上記第１装置から送信された第１装置の識別情報と鍵の属性情報と第１乱数とを受信し、第２装置において上記鍵の属性情報から鍵を計算し、第２装置において上記鍵と上記第１・第２乱数から第３乱数を発生し、第２・第３乱数と鍵に関する情報とを第２装置から第１装置に送信し、第１装置において上記第２装置から送信された第２・第３乱数と鍵に関する情報とを受信し、第１装置において上記鍵に関する情報から鍵を生成し、第１装置において上記鍵と上記第１・第２乱数から第４乱数を発生し、上記第４乱

数を第１装置から第２装置に送信し、第１・第２装置の各々において第３・第４乱数と鍵とから一時鍵を求めることを特徴とする。

また、本発明に係る認証方法は、第１装置において第１乱数を発生し、第１装置の識別情報と第１装置の鍵の属性情報と第２装置の鍵の属性情報と上記第１乱数とを第１装置から第２装置に送信し、第２装置において第２乱数を発生し、第２装置において上記第１装置から送信された第１装置の識別情報と鍵の属性情報と第２装置の鍵の属性情報と上記第１乱数とを受信し、第２装置において上記第２装置の鍵の属性情報から第１鍵を計算し、第２装置において上記第１装置の鍵の属性情報から第２鍵を計算し、第２装置において上記第２鍵と上記第１・第２乱数から第３乱数を発生し、第２・第３乱数と鍵に関する情報とを第２装置から第１装置に送信し、第１装置において上記第２装置から送信された第２・第３乱数と鍵に関する情報とを受信し、第１装置において上記鍵に関する情報から第２鍵を生成し、第１装置において上記第２鍵と上記第１・第２乱数から第４乱数を発生し、上記第４乱数を第１装置から第２装置に送信し、第１・第２装置の各々において第３・第４乱数と第２鍵とから一時鍵を求めることを特徴とする。

また、本発明は、暗号化されている所定のデータ及び前記所定のデータを暗号化している鍵を情報処理装置に提供する情報提供装置において、前記情報処理装置から、前記情報処理装置がダウンロードした前記データの利用に関するデータ及び決済に必要なデータを受信するとともに、前記情報処理装置に、前記鍵を送信する通信手段と、前記情報処理装置から受信した前記データの利用に関するデータ及び決済に必要なデータを基に、決済をする決済手段とを含む

ことを特徴とする。

また、本発明は、暗号化されている所定のデータ及び前記所定のデータを暗号化している鍵を情報処理装置に提供する情報提供方法において、前記情報処理装置から、前記情報処理装置がダウンロードした前記データの利用に関するデータ及び決済に必要なデータを受信するとともに、前記情報処理装置に、前記鍵を送信する通信ステップと、前記情報処理装置から受信した前記データの利用に関するデータ及び決済に必要なデータを基に、決済をする決済ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、暗号化されている所定のデータ及び前記所定のデータを暗号化している鍵を情報処理装置に提供する情報提供装置に、前記情報処理装置から、前記情報処理装置がダウンロードした前記データの利用に関するデータ及び決済に必要なデータを受信するとともに、前記情報処理装置に、前記鍵を送信する通信ステップと、前記情報処理装置から受信した前記データの利用に関するデータ及び決済に必要なデータを基に、決済をする決済ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明に係る情報処理装置は、暗号化されているプログラムを復号して実行する第１の実行手段と、前記プログラムを前記第１の実行手段に供給するとともに、暗号化されている前記プログラムを復号し、前記第１の実行手段の実行の結果を基に、前記プログラムを実行する第２の実行手段とを含むことを特徴とする。

また、本発明に係る情報処理方法は、暗号化されているプログラムを復号して実行する第１の実行ステップと、前記プログラムを前

記第１の実行ステップに供給するとともに、暗号化されている前記プログラムを復号し、前記第１の実行ステップの実行の結果を基に、前記プログラムを実行する第２の実行ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、暗号化されているプログラムを復号して実行する第１の実行ステップと、前記プログラムを前記第１の実行ステップに供給するとともに、暗号化されている前記プログラムを復号し、前記第１の実行ステップの実行の結果を基に、前記プログラムを実行する第２の実行ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置において、前記半導体ＩＣに実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信手段と、前記認証局から受信した、暗号化された前記プログラムを記録する記録手段と、前記記録手段に記録されている前記プログラムを、前記半導体ＩＣに送信する送信手段とを含むことを特徴とする。

また、本発明は、半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置の情報処理方法において、前記半導体ＩＣに実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信ステップと、前記認証局から受信した、暗号化された前記プログラムを記録する記録ステップと、前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップとを

含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置に、前記半導体ＩＣに実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信ステップと、前記認証局から受信した、暗号化された前記プログラムを記録する記録ステップと、前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置及び認証局からなる情報処理システムにおいて、前記情報処理装置は、前記半導体ＩＣに実行させる前記プログラムを認証局に送信するとともに、記認証局から暗号化された前記プログラムを受信する通信手段と、前記認証局から受信した、暗号化された前記プログラムを記録する記録手段と、前記記録手段に記録されている前記プログラムを、前記半導体ＩＣに送信する送信手段とを含み、前記認証局は、　前記半導体ＩＣに実行させる前記プログラムを受信するとともに、前記情報処理装置に暗号化された前記プログラムを送信する通信手段と、前記通信手段が受信した前記プログラムを所定の方式で暗号化する暗号化手段と含むことを特徴とする。

また、本発明は、半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置において、前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び

替え手段と、前記命令列が並び替えられた前記プログラムを記録する記録手段と、前記記録手段に記録されている前記プログラムを、前記半導体ＩＣに送信する送信手段とを含むことを特徴とする。

また、本発明は、半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置の情報処理方法において、前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、前記命令列が並び替えられた前記プログラムを記録する記録ステップと、前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置に、前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、前記命令列が並び替えられた前記プログラムを記録する記録ステップと、前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置において、前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替え手段と、前記プログラムを暗号化する暗号化手段と、前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録手段と、前記記録手段に記録されている前記プログラムを、前記半導体ＩＣに送信する送信手段とを含むことを特徴とする。

また、本発明は、半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置の情報処理方法において、前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、前記プログラムを暗号化する暗号化ステップと、前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録ステップと、前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置に、前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、前記プログラムを暗号化する暗号化ステップと、前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録ステップと、前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、情報処理装置に装着され、前記情報処理装置からの指令に基づいて、各種の処理を実行する半導体ＩＣにおいて、前記情報処理装置から転送されてくる暗号化されている第１のプログラムを受信する受信手段と、前記受信手段により受信された前記第１のプログラムを復号する復号手段と、前記復号手段により復号された前記第１のプログラムを処理する第２のプログラムを保持する保持手段と、前記保持手段に保持されている前記第２のプログラムに基づいて処理された前記第１のプログラムを実行する実行手段

と、前記実行手段が実行した結果を前記情報処理装置に転送する転送手段と、計時動作を行うとともに、前記情報処理装置からの時刻情報に基づいて、現在時刻を修正する計時手段とを含むことを特徴とする。

また、本発明は、情報処理装置に装着され、前記情報処理装置からの指令に基づいて、各種の処理を実行する半導体ＩＣの情報処理方法において、前記情報処理装置から転送されてくる暗号化されている第１のプログラムを受信する受信ステップと、前記受信ステップで受信された前記第１のプログラムを復号する復号ステップと、前記復号ステップで復号された前記第１のプログラムを処理する第２のプログラムを保持する保持ステップと、前記保持ステップの処理で保持された前記第２のプログラムに基づいて処理された前記第１のプログラムを実行する実行ステップと、前記実行ステップの処理で実行した結果を前記情報処理装置に転送する転送ステップと、計時動作を行うとともに、前記情報処理装置からの時刻情報に基づいて、現在時刻を修正する計時ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、情報処理装置に装着され、前記情報処理装置からの指令に基づいて、各種の処理を実行する半導体ICに、前記情報処理装置から転送されてくる暗号化されている第１のプログラムを受信する受信ステップと、前記受信ステップで受信された前記第１のプログラムを復号する復号ステップと、前記復号ステップで復号された前記第１のプログラムを処理する第２のプログラムを保持する保持ステップと、前記保持ステップの処理で保持された前記第２のプログラムに基づいて処理された前記第１のプログラムを実行する実行ステップと、前記実行ステップの処

理で実行した結果を前記情報処理装置に転送する転送ステップと、計時動作を行うとともに、前記情報処理装置からの時刻情報に基づいて、現在時刻を修正する計時ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、装着された半導体ICに各種の指令を出力し、実行させる情報処理装置において、前記半導体ＩＣに暗号化されているプログラムを送信する送信手段と、前記半導体ＩＣが、前記プログラムを処理した結果生成し、出力したデータを受信する第１の受信手段と、他の装置からデータと時刻情報を受信する第２の受信手段と、前記第２の受信手段が受信したデータを蓄積する蓄積手段と、前記第２の受信手段が受信した時刻情報に基づいて、前記半導体ＩＣの時刻情報を修正させる修正手段とを含むことを特徴とする。

また、本発明は、装着された半導体ＩＣに各種の指令を出力し、実行させる情報処理装置の情報処理方法において、前記半導体ＩＣに暗号化されているプログラムを送信する送信ステップと、前記半導体ＩＣが、前記プログラムを処理した結果生成し、出力したデータを受信する第１の受信ステップと、他の装置からデータと時刻情報を受信する第２の受信ステップと、前記第２の受信ステップで受信したデータを蓄積する蓄積ステップと、前記第２の受信ステップで受信した時刻情報に基づいて、前記半導体ＩＣの時刻情報を修正させる修正ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、装着された半導体ＩＣに各種の指令を出力し、実行させる情報処理装置に、前記半導体ＩＣに暗号化されているプログラムを送信する送信ステップと、前

記半導体ＩＣが、前記プログラムを処理した結果生成し、出力したデータを受信する第１の受信ステップと、他の装置からデータと時刻情報を受信する第２の受信ステップと、前記第２の受信ステップで受信したデータを蓄積する蓄積ステップと、前記第２の受信ステップで受信した時刻情報に基づいて、前記半導体ＩＣの時刻情報を修正させる修正ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、所定の半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置において、前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積手段と、前記蓄積手段に対する前記プログラム及び前記データの蓄積又は読み出しを制御する制御手段と、前記プログラムを前記半導体ＩＣから供給された第１の鍵で暗号化する第１の暗号化手段と、前記データを前記半導体ＩＣから供給された第２の鍵で暗号化する第２の暗号化手段とを含むことを特徴とする。

また、本発明は、所定の半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置の情報処理方法において、前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積ステップと、前記蓄積ステップで前記プログラム及び前記データの蓄積又は読み出しを制御する制御ステップと、前記プログラムを前記半導体ＩＣから供給された第１の鍵で暗号化する第１の暗号化ステップと、前記データを前記半導体ＩＣから供給された第２の鍵で暗号化する第２の暗号化ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、所定の半導体ＩＣが

装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置に、前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積ステップと、前記蓄積ステップで前記プログラム及び前記データの蓄積又は読み出しを制御する制御ステップと、前記プログラムを前記半導体ＩＣから供給された第１の鍵で暗号化する第１の暗号化ステップと、前記データを前記半導体ＩＣから供給された第２の鍵で暗号化する第２の暗号化ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

また、本発明は、所定の情報処理装置に装着し、前記情報処理装置から供給されたプログラム及び前記プログラムの実行に必要なデータを受信し、前記プログラムを実行する半導体ＩＣにおいて、前記半導体ＩＣ固有の第１の鍵を予め記憶している記憶手段と、前記記憶手段が記憶している前記第１の鍵及び前記情報処理装置から供給されたプログラムの属性から、第２の鍵を生成する鍵生成手段と、前記プログラムを第３の鍵で復号する第１の復号手段と、前記データを第２の鍵で復号する第２の復号手段とを含むことを特徴とする。

また、本発明は、所定の情報処理装置に装着し、前記情報処理装置から供給されたプログラム及び前記プログラムの実行に必要なデータを受信し、前記プログラムを実行する半導体ＩＣの情報処理方法において、前記半導体ＩＣ固有の第１の鍵を予め記憶している記憶ステップと、前記記憶ステップで記憶している前記第１の鍵及び前記情報処理装置から供給されたプログラムの属性から、第２の鍵を生成する鍵生成ステップと、前記プログラムを第３の鍵で復号する第１の復号ステップと、前記データを第２の鍵で復号する第２の

復号ステップとを含むことを特徴とする。

また、本発明に係るプログラム提供媒体は、所定の情報処理装置に装着し、前記情報処理装置から供給されたプログラム及び前記プログラムの実行に必要なデータを受信し、前記プログラムを実行する半導体ＩＣに、前記半導体ＩＣ固有の第１の鍵を予め記憶している記憶ステップと、前記記憶ステップで記憶している前記第１の鍵及び前記情報処理装置から供給されたプログラムの属性から、第２の鍵を生成する鍵生成ステップと、前記プログラムを第３の鍵で復号する第１の復号ステップと、前記データを第２の鍵で復号する第２の復号ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

さらに、本発明は、半導体ＩＣに実行させるプログラムを供給する情報処理装置及び前記情報処理装置に装着され、前記情報処理装置から供給されたプログラムを受信し、前記プログラムを実行する半導体ＩＣからなる情報処理システムにおいて、前記情報処理装置は、前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積手段と、前記蓄積手段に対する前記プログラム及び前記データの蓄積又は読み出しを制御する制御手段と、前記プログラムを前記半導体ＩＣから供給された第１の鍵で暗号化する第１の暗号化手段と、前記データを前記半導体ＩＣから供給された第２の鍵で暗号化する第２の暗号化手段と、暗号化された前記プログラム及び前記プログラムの実行に必要なデータを前記半導体ＩＣに送信するとともに、前記第１の鍵及び前記第２の鍵を前記半導体ＩＣから受信する第１の通信手段とを含み、前記半導体ＩＣは、暗号化された前記プログラム及び前記プログラムの実行に必要なデータを前記情

報処理装置から受信するとともに、前記第１の鍵及び前記第２の鍵を前記情報処理装置に送信する第２の通信手段と、前記半導体ＩＣ固有の第３の鍵を予め記憶している記憶手段と、前記記憶手段が記憶している前記第３の鍵及び前記情報処理装置から供給されたプログラムの属性から、第２の鍵を生成する鍵生成手段と、前記第２の通信手段が受信した、前記プログラムを第１の鍵で復号する第１の復号手段と、前記第２の通信手段が受信した、前記データを第２の鍵で復号する第２の復号手段とを含むことを特徴とする。

図面の簡単な説明

図１は、本発明を適用したコンテンツデータ管理システムの一実施の形態を示す図である。

図２は、上記コンテンツデータ管理システムにおけるパーソナルコンピュータの構成を説明する図である。

図３は、コンテンツデータ管理システムにおけるポータブルデバイスの構成を説明する図である。

図４は、上記パーソナルコンピュータの機能の構成を説明するブロック図である。

図５は、表示操作指示ウィンドウの例を示す図である。

図６は、録音プログラムがディスプレイに表示させるウィンドウの例を説明する図である。

図７は、コンパクトディスクからＨＤＤにコンテンツをコピーする場合の処理を説明するフローチャートである。

図８は、図７のフローチャートにおけるステップＳ１２の期限データベースチェック処理を説明するフローチャートである。

図９は、期限データベースの例を示す図である。

図１０は、ウォータマークを説明する図である。

図１１は、曲データベースの例を示す図である。

図１２は、ＨＤＤからポータブルデバイスへコンテンツを移動する動作を説明するフローチャートである。

図１３は、ＨＤＤからポータブルデバイスへコンテンツを移動する動作を説明するフローチャートである。

図１４は、ＨＤＤからポータブルデバイスへコンテンツを移動する動作を説明するフローチャートである。

図１５は、図１２のフローチャートにおけるステップＳ５５の選択されたコンテンツの再生条件などのチェック処理を説明するフローチャートである。

図１６は、ポータブルデバイス管理している再生条件を説明する図である。

図１７は、図１２のフローチャートにおけるステップＳ５８のフォーマット変換処理の詳細を説明するフローチャートである。

図１８は、ＨＤＤからポータブルデバイスへコンテンツをコピーする場合の動作を説明するフローチャートである。

図１９は、ＨＤＤからポータブルデバイスへコンテンツをコピーする場合の動作を説明するフローチャートである。

図２０は、ＨＤＤからポータブルデバイスへコンテンツをコピーする場合の動作を説明するフローチャートである。

図２１は、ポータブルデバイスからＨＤＤへコンテンツを移動す

る場合の動作を説明するフローチャートである。

図２２は、ポータブルデバイスからＨＤＤへコンテンツをコピーする場合の動作を説明フローチャートである。

図２３は、ＥＭＤサーバからＨＤＤへコンテンツをコピーする場合の処理を説明するフローチャートである。

図２４は、図２３のフローチャートにおけるステップＳ２０４の課金に関する処理の詳細を説明するフローチャートである。

図２５は、課金ログを説明する図である。

図２６は、パーソナルコンピュータのＩＥＣ６０９５８端子からＨＤＤへコンテンツをコピーする場合の処理を説明するフローチャートである。

図２７は、パーソナルコンピュータのＩＥＣ６０９５８端子からＨＤＤへコンテンツをコピーする場合の処理を説明するフローチャートである。

図２８は、ＨＤＤからＩＥＣ６０９５８端子にコンテンツを出力する場合の動作を説明するフローチャートである。

図２９は、ＨＤＤからＩＥＣ６０９５８端子にコンテンツを出力する場合の動作を説明するフローチャートである。

図３０は、図２８のフローチャートにおけるステップＳ２７５の再生条件などのチェック処理を説明するフローチャートである。

図３１は、ＨＤＤからポータブルデバイス経由でコンテンツを出力する場合の動作を説明するフローチャートである。

図３２は、ＨＤＤからポータブルデバイス経由でコンテンツを出力する場合の動作を説明するフローチャートである。

図３３は、不揮発性メモリの機能を説明する図である。

図３４は、アダプタの動作を説明するフローチャートである。

図３５は、アダプタの内部の構成を示す図である。

図３６Ａ及び図３６Ｂは、不揮発性メモリの内部の構成例を示す断面図である。

図３７は、不揮発性メモリの内部の構成例を示す斜視図である。

図３８は、アダプタとパーソナルコンピュータとの相互認証の処理を説明するフローチャートである。

図３９は、アダプタとパーソナルコンピュータとの相互認証の処理を説明するフローチャートである。

図４０は、アダプタとパーソナルコンピュータとの相互認証の処理を説明するフローチャートである。

図４１は、アダプタとパーソナルコンピュータとの相互認証の処理を説明するフローチャートである。

図４２は、ソースプログラムを暗号化する処理を説明するフローチャートである。

図４３は、暗号化されたソースプログラムをアダプタが実行する処理を説明するフローチャートである。

図４４は、オブジェクトプログラムを暗号化する処理を説明するフローチャートである。

図４５は、暗号化されたオブジェクトプログラムをアダプタが実行する処理を説明するフローチャートである。

図４６は、オブジェクトプログラムを暗号化する他の処理を説明するフローチャートである。

図４７は、暗号化されたオブジェクトプログラムをアダプタ７が実行する他の処理を説明するフローチャートである。

図４８は、アダプタがオブジェクトプログラムを実行する場合、処理の一部をパーソナルコンピュータのＣＰＵに実行させるときの処理を説明するフローチャートである。

図４９は、パーソナルコンピュータがＥＭＤサーバから暗号鍵をダウンロードするとともに、決済をする処理を説明するフローチャートである。

発明を実施するための最良の形態

以下、本発明を実施するための最良の形態について図面を参照しながら詳細に説明する。

図１は、本発明を適用したコンテンツデータ管理システムの一実施の形態を示す図である。パーソナルコンピュータ１は、ローカルエリアネットワーク又はインターネットなどから構成されるネットワーク２に接続されている。パーソナルコンピュータ１は、ＥＭＤ(Elecrical Music Distribution)サーバ４－１乃至４－３から受信した、又は後述するＣＤ(Compact Disc)から読み取った楽音のデータ（以下、コンテンツと称する）を、所定の圧縮の方式（例えば、ＡＴＲＡＣ３（商標））に変換するとともにＤＥＳ(Data Encryption Standard)などの暗号化方式で暗号化して記録する。

パーソナルコンピュータ１は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

利用条件のデータは、例えば、その利用条件のデータに対応する

コンテンツを同時に利用することができるポータブルデバイス(Portable Device(ＰＤとも称する))の台数（後述する、いわゆるチェックアウトできるＰＤの台数）を示す。利用条件のデータに示される数だけコンテンツをチェックアウトしたときでも、パーソナルコンピュータ１は、そのコンテンツを再生できる。

又は、利用条件のデータは、コピーすることができることを示す。コンテンツをポータブルデバイス６－１乃至６－３にコピーしたとき、パーソナルコンピュータ１は記録しているコンテンツを再生できる。コンテンツの、ポータブルデバイス６－１乃至６－３に記憶させることができる回数は、制限される場合がある。この場合、コピーできる回数は、増えることがない。

又は、利用条件のデータは、他のパーソナルコンピュータに移動することができるなどを示す。ポータブルデバイス６－１乃至６－３にコンテンツを移動させた後、パーソナルコンピュータ１が記録しているコンテンツは使用できなくなる（コンテンツが削除されるか、又は利用条件が変更されて使用できなくなる）。

利用条件のデータの詳細は、後述する。

パーソナルコンピュータ１は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ（例えば、曲名、又は再生条件など）とともに、ＵＳＢ(Universal Sirial Bus)ケーブル７－１を介して、接続されているポータブルデバイス６－１に記憶させるとともに、ポータブルデバイス６－１に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する（以下、チェックアウトと称する）。より詳細には、チェックアウトしたとき、パーソナルコンピュータ１が記録している、そのコンテン

ツに対応する利用条件のデータのチェックアウトできる回数は、１減らされる。チェックアウトできる回数が０のとき、対応するコンテンツは、チェックアウトすることができない。

パーソナルコンピュータ１は、暗号化して記録しているコンテンツを、コンテンツに関連するデータとともに、ＵＳＢケーブル７－２を介して、接続されているポータブルデバイス６－２に記憶させるとともに、ポータブルデバイス６－２に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ１は、暗号化して記録しているコンテンツを、コンテンツに関連するデータとともに、ＵＳＢケーブル７－３を介して、接続されているポータブルデバイス６－３に記憶させるとともに、ポータブルデバイス６－３に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。

また、パーソナルコンピュータ１は、ＵＳＢケーブル７－１を介して、接続されているポータブルデバイス６－１にパーソナルコンピュータ１がチェックアウトしたコンテンツを、ポータブルデバイス６－１に消去させて（又は、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する（以下、チェックインと称する）。より詳細には、チェックインしたとき、パーソナルコンピュータ１が記録している、対応するコンテンツの利用条件のデータのチェックアウトできる回数は、１増やされる。

パーソナルコンピュータ１は、ＵＳＢケーブル７－２を介して、接続されているポータブルデバイス６－２にパーソナルコンピュータ１がチェックアウトしたコンテンツを、ポータブルデバイス６－２に消去させて（又は、使用できなくさせて）、消去させたコンテ

ンツに対応する利用条件のデータを更新する。パーソナルコンピュータ１は、ＵＳＢケーブル７－３を介して、接続されているポータブルデバイス６－３にパーソナルコンピュータ１がチェックアウトしたコンテンツを、ポータブルデバイス６－３に消去させて（又は、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。

パーソナルコンピュータ１は、図示せぬ他のパーソナルコンピュータがポータブルデバイス６－１にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ１は、他のパーソナルコンピュータがポータブルデバイス６－２にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ１は、他のパーソナルコンピュータがポータブルデバイス６－３にチェックアウトしたコンテンツをチェックインできない。

ＥＭＤ登録サーバ３は、パーソナルコンピュータ１がＥＭＤサーバ４－１乃至４－３からコンテンツの取得を開始するとき、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、パーソナルコンピュータ１とＥＭＤサーバ４－１乃至４－３との相互認証に必要な認証鍵をパーソナルコンピュータ１に送信するとともに、ＥＭＤサーバ４－１乃至４－３に接続するためのプログラムをパーソナルコンピュータ１に送信する。

ＥＭＤサーバ４－１は、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、コンテンツに関連するデータ（例えば、曲名、又は再生制限など）とともに、パーソナルコンピュータ１にコンテンツを供給する。ＥＭＤサーバ４－２は、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、コン

テンツに関連するデータとともに、パーソナルコンピュータ１にコンテンツを供給する。ＥＭＤサーバ４－３は、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、コンテンツに関連するデータとともに、パーソナルコンピュータ１にコンテンツを供給する。

ＥＭＤサーバ４－１乃至４－３のそれぞれが供給するコンテンツは、同一又は異なる圧縮の方式で圧縮されている。ＥＭＤサーバ４－１乃至４－３のそれぞれが供給するコンテンツは、同一又は異なる暗号化の方式で暗号化されている。

ＷＷＷ(World Wide Web)サーバ５－１は、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、コンテンツを読み取ったＣＤ（例えば、ＣＤのアルバム名、又はＣＤの販売会社など）及びＣＤから読み取ったコンテンツに対応するデータ（例えば、曲名、又は作曲者名など）をパーソナルコンピュータ１に供給する。ＷＷＷサーバ５－２は、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、コンテンツを読み取ったＣＤ及びＣＤから読み取ったコンテンツに対応するデータをパーソナルコンピュータ１に供給する。

ポータブルデバイス６－１は、パーソナルコンピュータ１から供給されたコンテンツ（すなわち、チェックアウトされたコンテンツ）を、コンテンツに関連するデータ（例えば、曲名、又は再生制限など）とともに記憶する。ポータブルデバイス６－１は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。

例えば、コンテンツに関連するデータとして記憶されている、再

生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス６－１は、対応するコンテンツの再生を停止する。コンテンツに関連するデータとして記憶されている再生制限としての、再生期限を過ぎた後に再生しようとしたとき、ポータブルデバイス６－１は、対応するコンテンツの再生を停止する。

使用者は、コンテンツを記憶したポータブルデバイス６－１をパーソナルコンピュータ１から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

ポータブルデバイス６－２は、パーソナルコンピュータ１から供給されたコンテンツを、コンテンツに関連するデータとともに記憶する。ポータブルデバイス６－２は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス６－２をパーソナルコンピュータ１から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

ポータブルデバイス６－３は、パーソナルコンピュータ１から供給されたコンテンツを、コンテンツに関連するデータとともに記憶する。ポータブルデバイス６－３は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス６－３をパーソナルコンピュータ１から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

以下、ポータブルデバイス６－１乃至６－３を個々に区別する必要がないとき、単にポータブルデバイス６と称する。

図２は、パーソナルコンピュータ１の構成を説明する図である。ＣＰＵ(Central Processing Unit) １１は、各種アプリケーションプログラム（詳細については後述する）や、ＯＳ(Operating System)を実際に実行する。ＲＯＭ(Read-only Memory)１２は、一般的には、ＣＰＵ１１が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。ＲＡＭ（Ｒａｎｄｏｍ－Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１３は、ＣＰＵ１１の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはＣＰＵバスなどから構成されるホストバス１４により相互に接続されている。

ホストバス１４は、ブリッジ１５を介して、ＰＣＩ(Peripheral Component Interconnect/Interface) バスなどの外部バス１６に接続されている。

キーボード１８は、ＣＰＵ１１に各種の指令を入力するとき、使用者により操作される。マウス１９は、ディスプレイ２０の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ２０は、液晶表示装置又はＣＲＴ(Cathode Ray Tube)などから成り、各種情報をテキストやイメージで表示する。ＨＤＤ(Hard Disk Drive) ２１は、ハードディスクを駆動し、それらにＣＰＵ１１によって実行するプログラムや情報を記録又は再生させる。

ドライブ２２は、装着されている磁気ディスク４１、光ディスク４２（ＣＤを含む）、光磁気ディスク４３、又は半導体メモリ４４に記録されているデータ又はプログラムを読み出して、そのデータ

又はプログラムを、インターフェース１７、外部バス１６、ブリッジ１５及びホストバス１４を介して接続されているＲＡＭ１３に供給する。

ＵＳＢポート２３－１には、ＵＳＢケーブル７－１を介して、ポータブルデバイス６－１が接続される。ＵＳＢポート２３－１は、インターフェース１７、外部バス１６、ブリッジ１５、又はホストバス１４を介して、ＨＤＤ２１、ＣＰＵ１１、又はＲＡＭ１３から供給されたデータ（例えば、コンテンツ又はポータブルデバイス６－１のコマンドなどを含む）をポータブルデバイス６－１に出力する。

ＵＳＢポート２３－２には、ＵＳＢケーブル７－２を介して、ポータブルデバイス６－２が接続される。ＵＳＢポート２３－２は、インターフェース１７、外部バス１６、ブリッジ１５、又はホストバス１４を介して、ＨＤＤ２１、ＣＰＵ１１、又はＲＡＭ１３から供給されたデータ（例えば、コンテンツ又はポータブルデバイス６－２のコマンドなどを含む）をポータブルデバイス６－２に出力する。

ＵＳＢポート２３－３には、ＵＳＢケーブル７－３を介して、ポータブルデバイス６－３が接続される。ＵＳＢポート２３－３は、インターフェース１７、外部バス１６、ブリッジ１５、又はホストバス１４を介して、ＨＤＤ２１、ＣＰＵ１１、又はＲＡＭ１３から供給されたデータ（例えば、コンテンツ又はポータブルデバイス６－３のコマンドなどを含む）をポータブルデバイス６－３に出力する。

ＩＥＣ(Internationl Electrotechnical Commission)６０９５８

端子２４ａを有する音声入出力インターフェース２４は、デジタル音声入出力、あるいはアナログ音声入出力のインターフェース処理を実行する。スピーカ４５は、音声入出力インターフェース２４から供給された音声信号を基に、コンテンツに対応する所定の音声を出力する。

これらのキーボード１８乃至音声入出力インターフェース２４は、インターフェース１７に接続されており、インターフェース１７は、外部バス１６、ブリッジ１５及びホストバス１４を介してＣＰＵ１１に接続されている。

通信部２５は、ネットワーク２が接続され、ＣＰＵ１１、又はＨＤＤ２１から供給されたデータ（例えば、登録の要求、又はコンテンツの送信要求など）を、所定の方式のパケットに格納して、ネットワーク２を介して、送信するとともに、ネットワーク２を介して、受信したパケットに格納されているデータ（例えば、認証鍵、又はコンテンツなど）をＣＰＵ１１、ＲＡＭ１３、又はＨＤＤ２１に出力する。

半導体ＩＣとして、一体的に形成され、パーソナルコンピュータ１に装着されるアダプタ２６のＣＰＵ３２は、外部バス１６、ブリッジ１５及びホストバス１４を介してパーソナルコンピュータ１のＣＰＵ１１と共働し、各種の処理を実行する。ＲＡＭ３３は、ＣＰＵ３２が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ３４は、パーソナルコンピュータ１の電源がオフされた後も保持する必要があるデータを記憶する。ＲＯＭ３６には、パーソナルコンピュータ１から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記

憶されている。ＲＴＣ(Real Time Clock) ３５は、計時動作を実行し、時刻情報を提供する。

通信部２５及びアダプタ２６は、外部バス１６、ブリッジ１５及びホストバス１４を介してＣＰＵ１１に接続されている。

以下、ＵＳＢポート２３－１乃至２３－３を個々に区別する必要がないとき、単に、ＵＳＢポート２３と称する。以下、ＵＳＢケーブル７－１乃至７－３を個々に区別する必要がないとき、単にＵＳＢケーブル７と称する。

次に、ポータブルデバイス６の構成を図３を参照して説明する。電源回路５２は、乾電池５１から供給される電源電圧を所定の電圧の内部電力に変換して、ＣＰＵ５３乃至表示部６７に供給することにより、ポータブルデバイス６全体を駆動させる。

ＵＳＢコントローラ５７は、ＵＳＢコネクタ５６を介して、パーソナルコンピュータ１とＵＳＢケーブル７を介して接続された場合、パーソナルコンピュータ１から転送されたコンテンツを含むデータを、内部バス５８を介して、ＣＰＵ５３に供給する。

パーソナルコンピュータ１から転送されるデータは、１パケット当たり６４バイトのデータから構成され、１２Ｍｂｉｔ／ｓｅｃの転送レートでパーソナルコンピュータ１から転送される。

ポータブルデバイス６に転送されるデータは、ヘッダ及びコンテンツから構成される。ヘッダには、コンテンツＩＤ、ファイル名、ヘッダサイズ、コンテンツ鍵、ファイルサイズ、コーデックＩＤ、ファイル情報などが格納されているとともに、再生制限処理に必要な再生制限データ、開始日時、終了日時、回数制限及び再生回数カウンタなどが格納されている。コンテンツは、ＡＴＲＡＣ３などの

符号化方式で符号化され、暗号化されている。

ヘッダサイズは、ヘッダのデータ長（例えば、３３バイトなど）を表し、ファイルサイズは、コンテンツのデータ長（例えば、３３，６３６，１３８バイトなど）を表す。

コンテンツ鍵は、暗号化されているコンテンツを復号するための鍵であり、パーソナルコンピュータ１とポータブルデバイス６との相互認証の処理で生成されたセッション鍵（一時鍵）を基に暗号化された状態で、パーソナルコンピュータ１からポータブルデバイス６に送信される。

ポータブルデバイス６がＵＳＢケーブル７を介してパーソナルコンピュータ１のＵＳＢポート２３に接続されたとき、ポータブルデバイス６とパーソナルコンピュータ１とは、相互認証の処理を実行する。この相互認証の処理は、例えば、チャレンジレスポンス方式の認証の処理である。ちなみに、ポータブルデバイス６のＤＳＰ５９は、チャレンジレスポンス方式の認証の処理を行うとき、暗号解読（復号）の処理を実行する。

チャレンジレスポンス方式とは、例えば、パーソナルコンピュータ１が生成するある値（チャレンジ）に対して、ポータブルデバイス６がパーソナルコンピュータ１と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。チャレンジレスポンス方式の相互認証の処理においては、パーソナルコンピュータ１が生成する値は認証の処理毎に毎回変化するので、例えば、ポータブルデバイス６が出力した、秘密鍵を使用して生成された値が読み出されて、いわゆる、なりすましの攻撃を受けても、次の相互認証の処理では、相互認証に使用される値が異なるので、パーソナル

コンピュータ１は不正を検出できる。

コンテンツＩＤは、コンテンツに対応した、コンテンツを特定するためのＩＤである。

コーデックＩＤは、コンテンツの符号化方式に対応したＩＤであり、例えば、コーデックＩＤ”１”は、ＡＴＲＡＣ３に対応し、コーデックＩＤ”０”は、ＭＰ３(MPEG(Moving Picture Experts Group) Audio Layer-3)に対応する。

ファイル名は、コンテンツに対応するパーソナルコンピュータ１が記録しているコンテンツファイル（後述する）をＡＳＣＩＩ(American National Standard Code for Information Interchange)コードに変換したデータであり、ファイル情報は、コンテンツに対応する曲名、アーティスト名、作詞者名、又は作曲者名などをＡＳＣＩＩコードに変換したデータである。

再生制限データは、コンテンツの再生が可能な期間（すなわち、開始日時又は終了日時）又は回数制限（再生の回数の制限）が設定されているか否かを示すデータである。再生制限データには、回数制限が設定されているとき、”１”が割り当てられ、再生が可能な期間が設定されているとき、”２”が割り当てられ、回数制限及び再生が可能な期間がいずれも設定されていないとき（いわゆる、買取りで購入されたとき）、”０”が割り当てられる。

開始日時及び終了日時は、再生制限データが”２”であるとき、再生可能期間の範囲を示すデータである。例えば、開始日時が”０００４０Ｆ”であり、終了日時が”０００７０Ｆ”であるとき、対応するコンテンツは、２０００年４月１５日から２０００年７月１５日まで、再生が可能である。

同様に、回数制限及び再生回数カウンタは、再生制限データが”１”又は”２”であるとき、回数制限は、そのコンテンツに対応して予め設定された再生可能な回数であり、再生回数カウンタは、そのコンテンツの再生の処理を実行したときＣＰＵ５３により更新される、コンテンツが再生された回数を示す。例えば、回数制限が”０２”であるとき、そのコンテンツの再生可能な回数は２回であり、再生回数カウンタが”０１”であるとき、そのコンテンツが再生された回数は１回である。

例えば、再生制限データが”２”であり、開始日時が”０００４０Ｆ”であり、終了日時が”０００７０Ｆ”であり、回数制限が”０２”であるとき、ポータブルデバイス６は、対応するコンテンツを、２０００年４月１５日から２０００年７月１５日までの期間において、１日２回ずつ繰り返し再生できる。

例えば、再生制限データが”１”であり、開始日時が”０００００”であり、終了日時が”０００００”であり、回数制限が”０ａ”であり、再生回数カウンタが”０５”であるとき、対応するコンテンツは、再生可能な期間の制限がなく、再生可能な回数が１０回であり、再生された回数が５回である。

ポータブルデバイス６が、パーソナルコンピュータ１からコンテンツとともにコンテンツの書き込み命令を受信した場合、ＲＯＭ５５からＲＡＭ５４に読み出したメインプログラムを実行するＣＰＵ５３は、書き込み命令を受け取り、フラッシュメモリコントローラ６０を制御して、パーソナルコンピュータ１から受信したコンテンツをフラッシュメモリ６１に書き込ませる。

フラッシュメモリ６１は、約６４ＭＢｙｔｅの記憶容量を有し、

コンテンツを記憶する。また、フラッシュメモリ６１には、所定の圧縮方式で圧縮されているコンテンツを伸張するための再生用コードが予め格納されている。

なお、フラッシュメモリ６１は、ポータブルデバイス６にメモリカードとして着脱可能とすることができる。

使用者による、図示せぬ再生／停止ボタンの押し下げ操作に対応した再生命令が操作キーコントローラ６２を介してＣＰＵ５３に供給されると、ＣＰＵ５３は、フラッシュメモリコントローラ６０に、フラッシュメモリ６１から、再生用コードとコンテンツとを読み出させ、ＤＳＰ５９に転送させる。

ＤＳＰ５９は、フラッシュメモリ６１から転送された再生用コードに基づいてコンテンツをＣＲＣ(Cyclic Redundancy Check) 方式で誤り検出をした後、再生して、再生したデータ（図３中においてＤ１で示す）をディジタル／アナログ変換回路６３に供給する。

ＤＳＰ５９は、内部に設けられた図示せぬ発信回路とともに一体に構成され、外付けされた水晶で成る発信子５９Ａからのマスタークロック ＭＣＬＫを基に、コンテンツを再生するとともに、マスタークロック ＭＣＬＫ、マスタークロック ＭＣＬＫを基に内部の発振回路で生成した所定の周波数のビットクロック ＢＣＬＫ、並びに、フレーム単位のＬチャンネルクロック ＬＣＬＫ及びＲチャンネルクロック ＲＣＬＫからなる動作クロック ＬＲＣＬＫをディジタルアナログ変換回路６３に供給する。

ＤＳＰ５９は、コンテンツを再生するとき、再生用コードに従って上述の動作クロックをディジタルアナログ変換回路６３に供給して、コンテンツを再生しないとき、再生用コードに従って動作クロ

ックの供給を停止して、ディジタルアナログ変換回路６３を停止させて、ポータブルデバイス６全体の消費電力量を低減する。

同様に、ＣＰＵ５３及びＵＳＢコントローラ５７も、水晶でなる発振子５３Ａ又は５７Ａがそれぞれ外付けされ、発振子５３Ａ又は５７Ａからそれぞれ供給されるマスタークロックＭＣＬＫに基づき、所定の処理を実行する。

このように構成することで、ポータブルデバイス６は、ＣＰＵ５３，ＤＳＰ５９，ＵＳＢコントローラ５７等の各回路ブロックに対してクロック供給を行うためのクロック発生モジュールが不要となり、回路構成を簡素化するとともに小型化することができる。

ディジタルアナログ変換回路６３は、再生したコンテンツをアナログの音声信号に変換して、これを増幅回路６４に供給する。増幅回路６４は、音声信号を増幅して、ヘッドフォンジャック６５を介して、図示せぬヘッドフォンに音声信号を供給する。

このように、ポータブルデバイス６は、図示せぬ再生／停止ボタンが押圧操作されたとき、ＣＰＵ５３の制御に基づいてフラッシュメモリ６１に記憶されているコンテンツを再生するとともに、再生中に再生／停止ボタンが押圧操作されたとき、コンテンツの再生を停止する。

ポータブルデバイス６は、停止後に再度再生／停止ボタンが押圧操作されたとき、ＣＰＵ５３の制御に基づいて停止した位置からコンテンツの再生を再開する。再生／停止ボタンが押圧操作により再生を停止して操作が加わることなく数秒間経過したとき、ポータブルデバイス６は、自動的に電源をオフして消費電力を低減する。

因みに、ポータブルデバイス６は、電源がオフになった後に再生

／停止ボタンが押圧操作されたとき、前回の停止した位置からコンテンツを再生せず、１曲目から再生する。

また、ポータブルデバイス６のＣＰＵ５３は、ＬＣＤコントローラ６８を制御して、表示部６７に、再生モードの状態（例えば、リピート再生、イントロ再生など）、イコライザ調整（すなわち、音声信号の周波数帯域に対応した利得の調整）、曲番号、演奏時間、再生、停止、早送り、早戻しなどの状態、音量及び乾電池５１の残量等の情報を表示させる。

さらに、ポータブルデバイス６は、ＥＥＰＲＯＭ６８に、フラッシュメモリ８０に書き込まれているコンテンツの数、それぞれのコンテンツが書き込まれているフラッシュメモリ６１のブロック位置及びその他種々のメモリ蓄積情報等のいわゆるＦＡＴ（Ｆｉｌｅ Ａｌｌｏｃａｔｉｏｎ Ｔａｂｌｅ）を格納する。

因みに、本実施の形態においては、コンテンツは、６４ＫＢｙｔｅを１ブロックとして扱われ、１曲のコンテンツに対応したブロック位置がＦＡＴに格納される。

フラッシュメモリ６１にＦＡＴが格納される場合、例えば、１曲目のコンテンツがＣＰＵ５３の制御によりフラッシュメモリ６１に書き込まれると、１曲目のコンテンツに対応するブロック位置がＦＡＴとしてフラッシュメモリ６１に書き込まれ、次に、２曲目のコンテンツがフラッシュメモリ６１に書き込まれると、２曲目のコンテンツに対応するブロック位置がＦＡＴとしてフラッシュメモリ６１（１曲目と同一の領域）に書き込まれる。

このように、ＦＡＴは、フラッシュメモリ６１へのコンテンツの書き込みのたびに書き換えられ、更に、データの保護の為、同一の

データがリザーブ用に２重に書き込まれる。

ＦＡＴがフラッシュメモリ６１に書き込まれると、１回のコンテンツの書き込みに対応して、フラッシュメモリ６１の同一の領域が２回書き換えられるので、少ないコンテンツの書き込みの回数で、フラッシュメモリ６１に規定されている書換えの回数に達してしまい、フラッシュメモリ６１の書換えができなくなってしまう。

そこで、ポータブルデバイス６は、ＦＡＴをＥＥＰＲＯＭ６８に記憶させて、１回のコンテンツの書き込みに対応するフラッシュメモリ６１の書換えの頻度を少なくしている。

書換えの回数の多いＦＡＴをＥＥＰＲＯＭ６８に記憶させることにより、ＦＡＴをフラッシュメモリ６１に記憶させる場合に比較して、ポータブルデバイス６は、コンテンツの書き込みができる回数を数十倍以上に増やすことができる。更に、ＣＰＵ５３は、ＥＥＰＲＯＭ６８にＦＡＴを追記するように書き込ませるので、ＥＥＰＲＯＭ６８の同一の領域の書換えの頻度を少なくして、ＥＥＰＲＯＭ６８が短期間で書換え不能になることを防止する。

ポータブルデバイス６は、ＵＳＢケーブル７を介してパーソナルコンピュータ１に接続されたとき（以下、これをＵＳＢ接続と称する）、ＵＳＢコントローラ５７からＣＰＵ５３に供給される割り込み信号に基づき、ＵＳＢ接続されたことを認識する。

ポータブルデバイス６は、ＵＳＢ接続されたことを認識すると、パーソナルコンピュータ１からＵＳＢケーブル７を介して規定電流値の外部電力の供給を受けるとともに、電源回路５２を制御して、乾電池５１からの電力の供給を停止させる。

ＣＰＵ５３は、ＵＳＢ接続されたとき、ＤＳＰ５９のコンテンツ

の再生の処理を停止させる。これにより、ＣＰＵ５３は、パーソナルコンピュータ１から供給される外部電力が規定電流値を超えてしまうことを防止して、規定電流値の外部電力を常時受けられるように制御する。

このようにＣＰＵ５３は、ＵＳＢ接続されると、乾電池５１から供給される電力からパーソナルコンピュータ１から供給される電力に切り換えるので、電力単価の安いパーソナルコンピュータ１からの外部電力が使用され、電力単価の高い乾電池５１の消費電力が低減され、かくして乾電池５１の寿命を延ばすことができる。

なお、ＣＰＵ５３は、パーソナルコンピュータ１からＵＳＢケーブル７を介して外部電力の供給を受けたとき、ＤＳＰ５９の再生処理を停止させることにより、ＤＳＰ５９からの輻射を低減させ、その結果としてパーソナルコンピュータ１を含むシステム全体の輻射を一段と低減させる。

図４は、ＣＰＵ１１の所定のプログラムの実行等により実現される、パーソナルコンピュータ１の機能の構成を説明するブロック図である。コンテンツ管理プログラム１１１は、ＥＭＤ選択プログラム１３１、チェックイン／チェックアウト管理プログラム１３２、暗号方式変換プログラム１３５、圧縮方式変換プログラム１３６、暗号化プログラム１３７、利用条件変換プログラム１３９、利用条件管理プログラム１４０、認証プログラム１４１、復号プログラム１４２、ＰＤ用ドライバ１４３、購入用プログラム１４４及び購入用プログラム１４５などの複数のプログラムで構成されている。

コンテンツ管理プログラム１１１は、例えば、シャッフルされているインストラクション、又は暗号化されているインストラクショ

ンなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、コンテンツ管理プログラム１１１を読み出しても、インストラクションを特定できないなど）ように構成されている。

ＥＭＤ選択プログラム１３１は、コンテンツ管理プログラム１１１がパーソナルコンピュータ１にインストールされるとき、コンテンツ管理プログラム１１１には含まれず、後述するＥＭＤの登録の処理において、ネットワーク２を介して、ＥＭＤ登録サーバ３から受信される。ＥＭＤ選択プログラム１３１は、ＥＭＤサーバ４－１乃至４－３のいずれかとの接続を選択して、購入用アプリケーション１１５、又は購入用プログラム１４４若しくは１４２に、ＥＭＤサーバ４－１乃至４－３のいずれかとの通信（例えば、コンテンツを購入するときの、コンテンツのダウンロードなど）を実行させる。

チェックイン／チェックアウト管理プログラム１３２は、チェックイン又はチェックアウトの設定、及びコンテンツデータベース１１４に記録されている利用条件ファイル１６２－１乃至１６２－Ｎに基づいて、コンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツをポータブルデバイス６－１乃至６－３のいずれかにチェックアウトするか、又はポータブルデバイス６－１乃至６－３に記憶されているコンテンツをチェックインする。

チェックイン／チェックアウト管理プログラム１３２は、チェックイン又はチェックアウトの処理に対応して、コンテンツデータベース１１４に記録されている利用条件ファイル１６２－１乃至１６２－Ｎに格納されている利用条件のデータを更新する。

コピー管理プログラム１３３は、コンテンツデータベース１１４

に記録されている利用条件ファイル１６２－１乃至１６２－Ｎに基づいて、コンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツをポータブルデバイス６－１乃至６－３のいずれかにコピーするか、又はポータブルデバイス６－１乃至６－３からコンテンツをコンテンツデータベース１１４にコピーする。

移動管理プログラム１３４は、コンテンツデータベース１１４に記録されている利用条件ファイル１６２－１乃至１６２－Ｎに基づいて、コンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツをポータブルデバイス６－１乃至６－３のいずれかに移動するか、又はポータブルデバイス６－１乃至６－３からコンテンツをコンテンツデータベース１１４に移動する。

暗号方式変換プログラム１３５は、ネットワーク２を介して、購入用アプリケーションプログラム１１５がＥＭＤサーバ４－１から受信したコンテンツの暗号化の方式、購入用プログラム１４４がＥＭＤサーバ４－２から受信したコンテンツの暗号化の方式、又は購入用プログラム１４５がＥＭＤサーバ４－３から受信したコンテンツの暗号化の方式を、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツと同一の暗号化の方式に変換する。

また、暗号方式変換プログラム１３５は、ポータブルデバイス６－１又は６－３にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス６－１又は６－３が利用可能な暗号化方式に変換する。

圧縮方式変換プログラム１３６は、ネットワーク２を介して、購入用アプリケーションプログラム１１５がＥＭＤサーバ４－１から

受信したコンテンツの圧縮の方式、購入用プログラム１４４がＥＭＤサーバ４－２から受信したコンテンツの圧縮の方式、又は購入用プログラム１４５がＥＭＤサーバ４－３から受信したコンテンツの圧縮の方式を、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツと同一の圧縮の方式に変換する。

また、圧縮方式変換プログラム１３６は、ポータブルデバイス６－１又は６－３にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス６－１又は６－３が利用可能な圧縮の方式に変換する。

暗号化プログラム１３７は、例えばＣＤから読み取られ、録音プログラム１１３から供給されたコンテンツ（暗号化されていない）を、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツと同一の暗号化の方式で暗号化する。

圧縮／伸張プログラム１３８は、例えばＣＤから読み取られ、録音プログラム１１３から供給されたコンテンツ（圧縮されていない）を、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツと同一の符号化の方式で符号化する。圧縮／伸張プログラム１３８は、符号化されているコンテンツを伸張（復号）する。

利用条件変換プログラム１３９は、ネットワーク２を介して、購入用アプリケーションプログラム１１５がＥＭＤサーバ４－１から受信したコンテンツの利用条件を示すデータ（いわゆる、Ｕｓａｇｅ　Ｒｕｌｅ）、購入用プログラム１４４がＥＭＤサーバ４－２か

ら受信したコンテンツの利用条件を示すデータ、又は購入用プログラム１４５がＥＭＤサーバ４－３から受信したコンテンツの利用条件を示すデータを、コンテンツデータベース１１４が記録している利用条件ファイル１６２－１乃至１６２－Ｎに格納されている利用条件データと同一のフォーマットに変換する。

また、利用条件変換プログラム１３９は、ポータブルデバイス６－１又は６－３にコンテンツをチェックアウトするとき、チェックアウトするコンテンツに対応する利用条件のデータを、ポータブルデバイス６－１又は６－３が利用可能な利用条件のデータに変換する。

利用条件管理プログラム１４０は、コンテンツのコピー、移動、チェックイン、又はチェックアウトの処理を実行する前に、コンテンツデータベース１１４に記録されている利用条件ファイル１６２－１乃至１６２－Ｎに格納されている利用条件のデータに対応するハッシュ値（後述する）を基に、利用条件のデータの改竄を検出する。利用条件管理プログラム１４０は、コンテンツのコピー、移動、チェックイン、又はチェックアウトの処理に伴う、コンテンツデータベース１１４に記録されている利用条件ファイル１６２－１乃至１６２－Ｎに格納されている利用条件のデータを更新に対応して、利用条件のデータに対応するハッシュ値を更新する。

認証プログラム１４１は、コンテンツ管理プログラム１１１と購入用アプリケーションプログラム１１５との相互認証の処理及びコンテンツ管理プログラム１１１と購入用プログラム１４４との相互認証の処理を実行する。また、認証プログラム１４１は、ＥＭＤサーバ４－１と購入用アプリケーションプログラム１１５との相互認

証の処理、ＥＭＤサーバ４－２と購入用プログラム１４４との相互認証の処理及びＥＭＤサーバ４－３と購入用プログラム１４５との相互認証の処理で利用される認証鍵を記憶している。

認証プログラム１４１が相互認証の処理で利用する認証鍵は、コンテンツ管理プログラム１１１がパーソナルコンピュータ１にインストールされたとき、認証プログラム１４１に記憶されておらず、表示操作指示プログラム１１２により登録の処理が正常に実行されたとき、ＥＭＤ登録サーバ３から供給され、認証プログラム１４１に記憶される。

復号プログラム１４２は、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツをパーソナルコンピュータ１が再生するとき、コンテンツを復号する。

ＰＤ用ドライバ１４３は、ポータブルデバイス６－２に所定のコンテンツをチェックアウトするとき、又はポータブルデバイス６－２から所定のコンテンツをチェックインするとき、ポータブルデバイス６－２にコンテンツ又はポータブルデバイス６－２に所定の処理を実行させるコマンドを供給する。

ＰＤ用ドライバ１４３は、ポータブルデバイス６－１に所定のコンテンツをチェックアウトするとき、又はポータブルデバイス６－１から所定のコンテンツをチェックインするとき、デバイスドライバ１１６－１にコンテンツ、又はデバイスドライバ１１６－１に所定の処理を実行させるコマンドを供給する。

ＰＤ用ドライバ１４３は、ポータブルデバイス６－３に所定のコンテンツをチェックアウトするとき、又はポータブルデバイス６－

３から所定のコンテンツをチェックインするとき、デバイスドライバ１１６－２にコンテンツ、又はデバイスドライバ１１６－２に所定の処理を実行させるコマンドを供給する。

購入用プログラム１４４は、いわゆる、プラグインプログラムであり、コンテンツ管理プログラム１１１とともにインストールされ、ＥＭＤ登録サーバ３からネットワーク２を介して供給され、又は所定のＣＤに記録されて供給される。購入用プログラム１４４は、パーソナルコンピュータ１にインストールされたとき、コンテンツ管理プログラム１１１の有する所定の形式のインターフェースを介して、コンテンツ管理プログラム１１１とデータを送受信する。

購入用プログラム１４４は、例えば、シャッフルされているインストラクション、又は暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、購入用プログラム１４４を読み出しても、インストラクションを特定できないなど）ように構成されている。

購入用プログラム１４４は、ネットワーク２を介して、ＥＭＤサーバ４－２に所定のコンテンツの送信を要求するとともに、ＥＭＤサーバ４－２からコンテンツを受信する。また、購入用プログラム１４４は、ＥＭＤサーバ４－２からコンテンツを受信するとき、課金の処理を実行する。

購入用プログラム１４５は、コンテンツ管理プログラム１１１とともにインストールされるプログラムであり、ネットワーク２を介して、ＥＭＤサーバ４－３に所定のコンテンツの送信を要求するとともに、ＥＭＤサーバ４－３からコンテンツを受信する。また、購

入用プログラム１４５は、ＥＭＤサーバ４－３からコンテンツを受信するとき、課金の処理を実行する。

表示操作指示プログラム１１２は、フィルタリングデータファイル１８１、表示データファイル１８２、画像ファイル１８３－１乃至１８３－Ｋ、又は履歴データファイル１８４を基に、ディスプレイ２０に所定のウィンドウの画像を表示させ、キーボード１８又はマウス１９への操作を基に、コンテンツ管理プログラム１１１にチェックイン又はチェックアウトなどの処理の実行を指示する。

フィルタリングデータファイル１８１は、コンテンツデータベース１１４に記録されているコンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツそれぞれに重み付けをするためのデータを格納して、ＨＤＤ２１に記録されている。

表示データファイル１８２は、コンテンツデータベース１１４に記録されているコンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツに対応するデータを格納して、ＨＤＤ２１に記録されている。

画像ファイル１８３－１乃至１８３－Ｋは、コンテンツデータベース１１４に記録されているコンテンツファイル１６１－１乃至１６１－Ｎに対応する画像、又は後述するパッケージに対応する画像を格納して、ＨＤＤ２１に記録されている。

以下、画像ファイル１８３－１乃至１８３－Ｋを個々に区別する必要がないとき、単に、画像ファイル１８３と称する。

履歴データファイル１８４は、コンテンツデータベース１１４に記録されているコンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツがチェックアウトされた回数、チェックイ

ンされた回数、その日付などの履歴データを格納して、ＨＤＤ２１に記録されている。

表示操作指示プログラム１１２は、登録の処理のとき、ネットワーク２を介して、ＥＭＤ登録サーバ３に、予め記憶しているコンテンツ管理プログラム１１１のＩＤを送信するとともに、ＥＭＤ登録サーバ３から認証用鍵及びＥＭＤ選択プログラム１３１を受信して、コンテンツ管理プログラム１１１に認証用鍵及びＥＭＤ選択プログラム１３１を供給する。

録音プログラム１１３は、所定のウィンドウの画像を表示させて、キーボード１８又はマウス１９への操作を基に、ドライブ２２に装着された光ディスク４２であるＣＤからコンテンツの録音時間などのデータを読み出す。

録音プログラム１１３は、ＣＤに記録されているコンテンツの録音時間などを基に、ネットワーク２を介して、ＷＷＷサーバ５－１又は５－２にＣＤに対応するデータ（例えば、アルバム名、又はアーティスト名など）又はＣＤに記録されているコンテンツに対応するデータ（例えば、曲名など）の送信を要求するとともに、ＷＷＷサーバ５－１又は５－２からＣＤに対応するデータ又はＣＤに記録されているコンテンツに対応するデータを受信する。

録音プログラム１１３は、受信したＣＤに対応するデータ又はＣＤに記録されているコンテンツに対応するデータを、表示操作指示プログラム１１２に供給する。

また、録音の指示が入力されたとき、録音プログラム１１３は、ドライブ２２に装着された光ディスク４２であるＣＤからコンテンツを読み出して、コンテンツ管理プログラム１１１に出力する。

コンテンツデータベース１１４は、コンテンツ管理プログラム１１１から供給された所定の方式で圧縮され、所定の方式で暗号化されているコンテンツを、コンテンツファイル１６１－１乃至１６１－Ｎのいずれかに格納する（ＨＤＤ２１に記録する）。コンテンツデータベース１１４は、コンテンツファイル１６１－１乃至１６１－Ｎにそれぞれ格納されているコンテンツに対応する利用条件のデータを、コンテンツが格納されているコンテンツファイル１６１－１乃至１６１－Ｎにそれぞれ対応する利用条件ファイル１６２－１乃至１６２－Ｎのいずれかに格納する（ＨＤＤ２１に記録する）。

コンテンツデータベース１１４は、コンテンツファイル１６１－１乃至１６１－Ｎ又は利用条件ファイル１６２－１乃至１６２－Ｎをレコードとして記録してもよい。

例えば、コンテンツファイル１６１－１に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル１６２－１に格納されている。コンテンツファイル１６１－Ｎに格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル１６２－Ｎに格納されている。

なお、利用条件ファイル１６２－１乃至１６２－Ｎに記録されているデータは、後述する期限データベースに記録されているデータ、又は曲データベースに記録されているデータに対応する。すなわち、コンテンツデータベース１１４は、後述する期限データベース及び曲データベースを包含して、構成されている。

以下、コンテンツファイル１６１－１乃至１６１－Ｎを個々に区別する必要がないとき、単に、コンテンツファイル１６１と称する。以下、利用条件ファイル１６２－１乃至１６２－Ｎを個々に区別す

る必要がないとき、単に、利用条件ファイル１６２と称する。

購入用アプリケーションプログラム１１５は、ＥＭＤ登録サーバ３からネットワーク２を介して供給され、又は所定のＣＤ－ＲＯＭに記録されて供給される。購入用アプリケーションプログラム１１５は、ネットワーク２を介して、ＥＭＤサーバ４－１に所定のコンテンツの送信を要求するとともに、ＥＭＤサーバ４－１からコンテンツを受信して、コンテンツ管理プログラム１１１に供給する。また、購入用アプリケーションプログラム１１５は、ＥＭＤサーバ４－１からコンテンツを受信するとき、課金の処理を実行する。

次に、表示データファイル８２に格納されているデータとコンテンツデータベースに格納されているコンテンツファイル１６１－１乃至１６１－Ｎとの対応付けについて説明する。

コンテンツファイル１６１－１乃至１６１－Ｎのいずれかに格納されているコンテンツは、所定のパッケージに属する。パッケージは、より詳細には、オリジナルパッケージ、マイセレクトパッケージ、又はフィルタリングパッケージのいずれかである。

オリジナルパッケージは、１以上のコンテンツが属し、ＥＭＤサーバ４－１乃至４－３におけるコンテンツの分類（例えば、いわゆるアルバムに対応する）、又は一枚のＣＤに対応する。コンテンツは、いずれかのオリジナルパッケージに属し、複数のオリジナルパッケージに属することができない。また、コンテンツが属するオリジナルパッケージは、変更することができない。使用者は、オリジナルパッケージに対応する情報の一部を編集（情報の追加、又は追加した情報の変更）することができる。

マイセレクトパッケージは、使用者が任意に選択した１以上のコ

ンテンツが属する。マイセレクトパッケージにいずれのコンテンツが属するかは、使用者が任意に編集することができる。コンテンツは、１以上のマイセレクトパッケージに同時に属することができる。また、コンテンツは、いずれのマイセレクトパッケージに属しなくともよい。

フィルタリングパッケージには、フィルタリングデータファイル１８１に格納されているフィルタリングデータを基に選択されたコンテンツが属する。フィルタリングデータは、ＥＭＤサーバ４－１乃至４－３又はＷＷＷサーバ５－１若しくは５－２などからネットワーク２を介して供給され、又は所定のＣＤに記録されて供給される。使用者は、フィルタリングデータファイル１８１に格納されているフィルタリングデータを編集することができる。

フィルタリングデータは、所定のコンテンツを選択する、又はコンテンツに対応する重みを算出する基準となる。例えば、今週のＪ－ＰＯＰ（日本のポップス）ベストテンに対応するフィルタリングデータを利用すれば、パーソナルコンピュータ１は、今週の日本のポップス１位のコンテンツ乃至今週の日本のポップス１０位のコンテンツを特定することができる。

フィルタリングデータファイル１８１は、例えば、過去１月間にチェックアウトされていた期間が長い順にコンテンツを選択するフィルタリングデータ、過去半年間にチェックアウトされた回数が多いコンテンツを選択するフィルタリングデータ、又は曲名に”愛”の文字が含まれているコンテンツを選択するフィルタリングデータなどを含んでいる。

このようにフィルタリングパッケージのコンテンツは、コンテン

ツに対応するコンテンツ用表示データ２２１（コンテンツ用表示データ２２１に使用者が設定したデータを含む）、又は履歴データ１８４などと、フィルタリングデータとを対応させて選択される。

ドライバ１１７は、コンテンツ管理プログラム１１１などの制御の基に、音声入出力インターフェース２４を駆動して、外部から供給されたデジタルデータであるコンテンツを入力してコンテンツ管理プログラム１１１に供給するか、若しくはコンテンツ管理プログラム１１１を介してコンテンツデータベース１１４から供給されたコンテンツをデジタルデータとして出力するか、又は、コンテンツ管理プログラム１１１を介してコンテンツデータベース１１４から供給されたコンテンツに対応するアナログ信号を出力する。

図５は、表示操作指示プログラム１１２を起動させたとき、操作指示プログラム１１２がディスプレイ２０に表示させる表示操作指示ウィンドウの例を示す図である。

表示操作指示ウィンドウには、録音プログラム１１３を起動させるためのボタン２０１、ＥＭＤ選択プログラム１３１を起動させるためのボタン２０２、チェックイン又はチェックアウトの処理の設定を行うフィールドを表示させるためのボタン２０３、マイセレクトパッケージを編集するためフィールドを表示させるためのボタン２０４等が配置されている。

ボタン２０５が選択されているとき、フィールド２１１には、オリジナルパッケージに対応するデータが表示される。ボタン２０６が選択されているとき、フィールド２１１には、マイセレクトパッケージに対応するデータが表示される。ボタン２０７が選択されているとき、フィールド２１１には、フィルタリングパッケージに対

応するデータが表示される。

フィールド２１１に表示されるデータは、パッケージに関するデータであり、例えば、パッケージ名称、又はアーティスト名などである。

例えば、図５においては、パッケージ名称”ファースト”及びアーティスト名”Ａ太郎”、パッケージ名称”セカンド”及びアーティスト名”Ａ太郎”などがフィールド２１１に表示される。

フィールド２１２には、フィールド２１１で選択されているパッケージに属するコンテンツに対応するデータが表示される。フィールド２１２に表示されるデータは、例えば、曲名、演奏時間、又はチェックアウト可能回数などである。

例えば、図５においては、パッケージ名称”セカンド”に対応するパッケージが選択されているので、パッケージ名称”セカンド”に対応するパッケージに属するコンテンツに対応する曲名”南の酒場”及びチェックアウト可能回数（例えば、８分音符の１つがチェックアウト１回に相当し、８分音符が２つでチェックアウト２回を示す）、並びに曲名”北の墓場”及びチェックアウト可能回数（８分音符が１つでチェックアウト１回を示す）などがフィールド２１２に表示される。

このように、フィールド２１２に表示されるチェックアウト可能回数としての１つの８分音符は、対応するコンテンツが１回チェックアウトできることを示す。

フィールド２１２に表示されるチェックアウト可能回数としての休符は、対応するコンテンツがチェックアウトできない（チェックアウト可能回数が０である。（ただし、パーソナルコンピュータ１

はそのコンテンツを再生することができる。））ことを示す。また、フィールド２１２に表示されるチェックアウト可能回数としてのト音記号は、対応するコンテンツのチェックアウトの回数に制限がない（何度でも、チェックアウトできる）ことを示している。

なお、チェックアウト可能回数は、図５に示すように所定の図形（例えば、円、星、月などでもよい）の数で表示するだけでなく、数字等で表示してもよい。

また、表示操作指示ウィンドウには、選択されているパッケージ又はコンテンツに対応付けられている画像等（図４の画像ファイル１８３－１乃至１８３－Ｋのいずれかに対応する）を表示させるフィールド２０８が配置されている。ボタン２０９は、選択されているコンテンツを再生する（コンテンツに対応する音声をスピーカ４５に出力させる）とき、クリックされる。

ボタン２０５が選択され、フィールド２１１に、オリジナルパッケージに対応するデータが表示されている場合、フィールド２１２に表示されている所定のコンテンツの曲名を選択して、消去の操作をしたとき、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１に、選択されている曲名に対応する、コンテンツデータベース１１４に格納されている所定のコンテンツを消去させる。

録音プログラム１１３が表示させるウィンドウのボタン（後述するボタン２５５）が選択されて（アクティブにされて）いる場合、ＣＤから読み出したコンテンツがコンテンツデータベース１１４に記録されたとき、表示操作指示プログラム１１２は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス６－１乃至６－３のいずれかに記憶されているコンテンツの曲名を表示するフ

ィールド２１３を表示する。

録音プログラム１１３が表示させるウィンドウのボタンが選択されている場合、ＣＤから読み出したコンテンツがコンテンツデータベース１１４に記録されたとき、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１に、コンテンツデータベース１１４に記録した、ＣＤから読み出したコンテンツを予め指定されているポータブルデバイス６－１乃至６－３のいずれかにチェックアウトさせる。

フィールド２１３にはコンテンツの曲名に対応させて、フィールド２１３の最も左に、そのコンテンツがパーソナルコンピュータ１にチェックインできるか否かを示す記号が表示される。例えば、フィールド２１３の最も左に位置する“○”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ１にチェックインできる（すなわち、パーソナルコンピュータ１からチェックアウトされた）ことを示している。フィールド２１３の最も左に位置する“×”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ１にチェックインできない（すなわち、パーソナルコンピュータ１からチェックアウトされていない、例えば、他のパーソナルコンピュータからチェックアウトされた）ことを示している。

表示操作指示プログラム１１２が表示操作指示ウィンドウにフィールド２１３を表示させたとき、表示操作指示プログラム１１２は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス６－１乃至６－３のいずれかに記憶されているコンテンツが属するポータブルパッケージ（ポータブルデバイス６－１乃至６－３のいずれかに記憶されているコンテンツが属するパーケージ）の名称

を表示するフィールド２１４、フィールド２１３を閉じるためのボタン２１０及びチェックイン又はチェックアウトを実行させるボタン２１５を表示する。

更に、表示操作指示プログラム１１２が表示操作指示ウィンドウにフィールド２１３を表示させたとき、表示操作指示プログラム１１２は、表示操作指示ウィンドウに、フィールド２１２で選択された曲名に対応するコンテンツのチェックアウトを設定するボタン２１６、フィールド２１３で選択された曲名に対応するコンテンツのチェックインを設定するボタン２１７、フィールド２１３に表示されたコンテンツ名に対応する全てのコンテンツのチェックインを設定するボタン２１８及びチェックイン又はチェックアウトの設定を取り消すボタン２１９を配置させる。

ボタン２１６乃至２１９の操作によるチェックイン又はチェックアウトの設定だけでは、パーソナルコンピュータ１は、チェックイン又はチェックアウトの処理を実行しない。

ボタン２１６乃至２１９の操作によるチェックイン又はチェックアウトの設定をした後、ボタン２１５がクリックされたとき、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１にチェックイン又はチェックアウトの処理を実行させる。すなわち、ボタン２１５がクリックされたとき、表示操作指示プログラム１１２は、チェックイン又はチェックアウトの設定に基づき、コンテンツ管理プログラム１１１に、ポータブルデバイス６－１乃至６－３のいずれかにコンテンツを送信させるか、又はチェックインに対応する所定のコマンド（例えば、ポータブルデバイス６－１乃至６－３のいずれかが記憶している所定のコンテンツを消去させるコマン

ドなど）を送信させるとともに、送信したコンテンツ又はコマンドに対応する利用条件ファイル１６２に格納されている利用条件のデータを更新させる。

チェックイン又はチェックアウトが実行されたとき、表示操作指示プログラム１１２は、送信したコンテンツ又は送信されたコマンドに対応して、履歴データファイル１８４に格納されている履歴データを更新する。履歴データは、チェックイン又はチェックアウトされたコンテンツを特定する情報、又はそのコンテンツがチェックイン又はチェックアウトされた日付、そのコンテンツがチェックアウトされたポータブルデバイス６－１乃至６－３の名称などから成る。

チェックイン又はチェックアウトの設定の処理は短時間で実行できるので、使用者は、チェックイン又はチェックアウトの処理の実行後の状態を迅速に知ることができ、時間のかかるチェックイン又はチェックアウトの処理の回数を減らして、チェックイン又はチェックアウトに必要な時間全体（設定及び実行を含む）を短くすることができる。

図６は、録音プログラム１１３がディスプレイ２０に表示させるウィンドウの例を説明する図である。例えば、ＷＷＷサーバ５－２から受信したＣＤの情報を基に、録音プログラム１１３は、フィールド２５１に、”アシンクロナイズド”などのＣＤのタイトルを表示する。ＷＷＷサーバ５－２から受信したＣＤの情報を基に、録音プログラム１１３は、フィールド２５２に、例えば、”クワイ”などのアーティスト名を表示する。

ＷＷＷサーバ５－２から受信したＣＤの情報を基に、録音プログ

ラム１１３は、フィールド２５３の曲名を表示する部分に、例えば、”ヒート”，”プラネット”，”ブラック”，”ソウル”などの曲名を表示する。同様に、録音プログラム１１３は、フィールド２５３のアーティストを表示する部分に、例えば、”クワイ”などのアーティスト名を表示する。

録音プログラム１１３が所定のＣＤの情報を受信した後、録音プログラム１１３は、ＨＤＤ２１の所定のディレクトリにＣＤの情報を格納する。

ボタン２５４などがクリックされて、ＣＤの情報の取得の指示を受けたとき、録音プログラム１１３は、始めに、ＨＤＤ２１の所定のディレクトリを検索する。録音プログラム１１３は、そのディレクトリにＣＤの情報が格納されているとき、図示せぬダイアログボックスを表示して、使用者にディレクトリに格納されているＣＤの情報を利用するか否かを選択させる。

録音プログラム１１３が表示させるウィンドウに配置されているコンテンツの録音の開始を指示するボタン２５６がクリックされたとき、録音プログラム１１３は、ドライブ２２に格納されているＣＤからコンテンツを読み出して、ＣＤから読み出したコンテンツをＣＤの情報とともにコンテンツ管理プログラム１１１に供給する。コンテンツ管理プログラム１１１の圧縮／伸張プログラム１３８は、録音プログラム１１３から供給されたコンテンツを所定の圧縮の方式で圧縮して、暗号化プログラム１３７は、圧縮されたコンテンツを、暗号化する。また、利用条件変換プログラム１３９は、圧縮され、暗号化されたコンテンツに対応する利用条件のデータを生成する。

コンテンツ管理プログラム１１１は、圧縮され、暗号化されたコンテンツを利用条件のデータとともに、コンテンツデータベース１１４に供給する。

コンテンツデータベース１１４は、コンテンツ管理プログラム１１１から受信したコンテンツに対応するコンテンツファイル１６１及び利用条件ファイル１６２を生成して、コンテンツファイル１６１にコンテンツを格納するとともに、利用条件ファイル１６２に利用条件のデータを格納する。

コンテンツ管理プログラム１１１は、コンテンツデータベース１１４にコンテンツ及びコンテンツに対応する利用条件のデータが格納されたとき、録音プログラム１１３から受信したＣＤの情報及び利用条件のデータを表示操作指示プログラム１１２に供給する。

表示操作指示プログラム１１２は、録音の処理でコンテンツデータベース１１４に格納されたコンテンツに対応する利用条件のデータ及びＣＤの情報を基に、表示データファイル１８２に格納する表示用のデータを生成する。

録音プログラム１１３が表示させるウィンドウには、更に、ＣＤから読み出したコンテンツをコンテンツデータベース１１４に記録したとき、自動的に、ＣＤから読み出したコンテンツをポータブルデバイス６－１乃至６－３のいずれかにチェックアウトさせるか否かの設定を行うボタン２５５が配置されている。

例えば、ボタン２５５がクリックされたとき、録音プログラム１１３は、ポータブルデバイス６－１乃至６－３のリストを示すプルダウンメニューを表示する。使用者が、そのプルダウンメニューからポータブルデバイス６－１乃至６－３のいずれかを選択したとき、

パーソナルコンピュータ１は、選択されたポータブルデバイス６－１乃至６－３のいずれかに、自動的に、ＣＤから記録したコンテンツをチェックアウトする。使用者が、そのプルダウンメニューから”チェックアウトしない”を選択した場合、パーソナルコンピュータ１は、ＣＤからコンテンツを記録したとき、チェックアウトしない。

このように、録音プログラム１１３が表示させるウィンドウのボタン２５５をアクティブにしておくだけで、ＣＤから読み出したコンテンツがコンテンツデータベース１１４に記録されたとき、パーソナルコンピュータ１は、予め指定されているポータブルデバイス６－１乃至６－３のいずれかに、ＣＤから読み出したコンテンツをチェックアウトさせることができる。

次に、図７のフローチャートを参照して、コンテンツ管理プログラム１１１、表示操作指示プログラム１１２、録音プログラム１１３、及びコンテンツデータベース１１４を実行するＣＰＵ１１による、ドライブ２２に装着されたＣＤから再生したコンテンツをＨＤＤ２１に転送し、コピーする場合の処理について説明する。使用者がキーボード１８又はマウス１９を操作して、インターフェース１７を介してＣＰＵ１１に対してドライブ２２に装着されたＣＤ（図示せず）から再生されたコンテンツをＨＤＤ２１に転送、コピーする指令を入力すると、録音プログラム１１３は、ステップＳ１１において、インターフェース１７を介してディスプレイ２０にコピーするコンテンツを選択するための、例えば、図６に示すＧＵＩ(Graphical User Interface)を表示させる。

具体的には、例えば、録音プログラム１１３は、ドライブ２２に

装着されたＣＤのＴＯＣ(Table Of Contents) を読み込み、そのＣＤに含まれるコンテンツの情報を得て、ディスプレイ２０に表示させる。又は、録音プログラム１１３は、ＣＤに含まれている各コンテンツ毎のＩＳＲＣ(International Standard Recording Code) を読み出し、そのコンテンツの情報を得て、ディスプレイ２０に表示させる。あるいはまた、ボタン２５４がクリックされたとき、録音プログラム１１３は、ネットワーク２を介してＷＷＷサーバ５－１又は５－２にアクセスし、ＴＯＣを用いて、そのＣＤのコンテンツの情報を得て、コンテンツに対応する曲名などをフィールド２５３に表示させる。

使用者は、ディスプレイ２０のＧＵＩを利用してキーボード１８又はマウス１９を操作し、フィールド２５３に表示されている曲名に対応するチェックボックスをクリックするなどして、コピーするコンテンツを選択する。

次に、ステップＳ１２において、録音プログラム１１３は、利用条件管理プログラム１４０に、ＨＤＤ２１に格納されている期限データベース（図４に示すコンテンツデータベース１１４の利用条件ファイル１６２－１乃至１６２－Ｎに対応する）をチェックさせる。この期限データベースチェック処理の詳細は、図８のフローチャートに示されている。

ステップＳ３１において利用条件管理プログラム１４０は、アダプタ２６のＣＰＵ３２と共働して、期限データベース全体のハッシュ値を計算し、ステップＳ３２において、その計算された値と、前回保存しておいたハッシュ値と比較する。

なお、期限データベースにデータが何ら記録されていないとき、

利用条件管理プログラム１４０は、ハッシュ値を計算しない。

すなわち、ＨＤＤ２１には、期限データベースが形成されており、この期限データベースには、図９に示すように、ＨＤＤ２１に記録されているコンテンツ（コンテンツ）を管理する管理情報として、過去に記録されたことのあるコンテンツのＩＳＲＣとコピー日時が対応して記憶されている。この例においては、アイテム１乃至アイテム３の３つのアイテムについて、それぞれのＩＳＲＣとコピー日時が記憶されている。この期限データベースに記録されている全てのコンテンツのＩＳＲＣとコピー日時に基づいた期限データベース全体のハッシュ値が、後述するように、ステップＳ３８において、アダプタ２６のＣＰＵ３２により計算され、不揮発性メモリ３４に記憶されている。ハッシュ値は、データに対してハッシュ関数を適用して得られた値である。ハッシュ関数は、一般的に可変長の長いデータを、固定長の短い値にマップする一方向性の関数であり、ハッシュ値同士の衝突が起こりにくい性質を有している。ハッシュ関数の例としては、ＳＨＡ(Secure Hash Algorithm)，ＭＤ(Message Digest)５などがある。利用条件管理プログラム１４０は、ステップＳ３１において、ＣＰＵ３２が実行したのと同様にハッシュ値を計算する。そして、ステップＳ３２において、利用条件管理プログラム１４０は、ＣＰＵ３２に、不揮発性メモリ３４に記憶されているハッシュ値の読み出しを要求し、転送を受けたハッシュ値と、ステップＳ３１で、いま自分自身が計算したハッシュ値とを比較する。

ステップＳ３３において、利用条件管理プログラム１４０は、ステップＳ３１でいま計算したハッシュ値と、不揮発性メモリ３４に記憶されている前回の期限データベースのハッシュ値とが一致する

か否かを判定し、一致しない場合には、期限データベースが改竄されたものと判定し、利用条件管理プログラム１４０は、ステップＳ３４において、例えば、録音プログラム１１３に「期限データベースが改竄されたので、コピーができません」といったメッセージを発生させ、インターフェース１７を介してディスプレイ２０に出力させ、表示させ、以後、処理を終了させる。すなわち、この場合には、ＣＤに記録されているコンテンツを再生し、ＨＤＤ２１にコピーする処理が禁止される。

ステップＳ３１で計算したハッシュ値と、前回のハッシュ値とが一致する場合には、ステップＳ３５に進み、利用条件管理プログラム１４０は、録音プログラム１１３に、ステップＳ１１で指定されたコピーするコンテンツとして選択されたコンテンツ（選択されたコンテンツ）のＩＳＲＣをＣＤから取得させる。ＣＤにＩＳＲＣが記録されていない場合、利用条件管理プログラム１４０は、録音プログラム１１３に、そのＣＤのＴＯＣのデータを読み出させ、そのデータにハッシュ関数を適用するなどして、例えば、５８ビットなどの適当な長さのデータを得て、これをＩＳＲＣに代えて用いる。

ステップＳ３６において、利用条件管理プログラム１４０は、ステップＳ３５で取得したＩＳＲＣ（すなわち、選択されたコンテンツ）が期限データベース（図９）に登録されているか否かを判定する。ＩＳＲＣが期限データベースに登録されていない場合には、そのコンテンツはまだＨＤＤ２１に記録されていないことになるので、ステップＳ３７に進み、利用条件管理プログラム１４０は、そのコンテンツのＩＳＲＣと現在の日時とを期限データベースに登録する。なお、利用条件管理プログラム１４０は、この現在の日時として、

ＣＰＵ３２から転送を受けた、アダプタ２６のＲＴＣ３５が出力する値を利用する。そして、ステップＳ３８において、利用条件管理プログラム１４０は、その時点における期限データベースのデータを読み出し、アダプタ２６のＣＰＵ３２に転送する。ＣＰＵ３２は、転送されてきたデータのハッシュ値を計算し、不揮発性メモリ３４に保存してする。上述したように、このようにして保存されたハッシュ値が、ステップＳ３２において、前回保存しておいたハッシュ値として利用される。

次に、ステップＳ３９において、利用条件管理プログラム１４０は、選択されたコンテンツが期限データベースに登録されていないことを表す未登録のフラグを設定する。このフラグは、後述する図７のステップＳ１３において、選択されたコンテンツが期限データベースに登録されているか否かの判定を行うときに用いられる。

ステップＳ３６において、選択されたコンテンツのＩＳＲＣが期限データベースに登録されていると判定された場合、その選択されたコンテンツは、少なくとも一度、ＨＤＤ２１に登録されたことがあるコンテンツであるということになる。そこで、この場合、ステップＳ４０に進み、利用条件管理プログラム１４０は、期限データベースに登録されているその選択されたコンテンツの登録日時より、現在の日時（アダプタ２６のＲＴＣ３５が出力した現在の日時）が４８時間以上経過しているか否かを判定する。現在時刻が、登録日時より、既に４８時間以上経過している場合には、ＨＤＤ２１に、少なくとも一度は記録したことがあるが、既に、その時から４８時間以上経過しているので、そのコンテンツを再度コピーさせたとしても、コンテンツの大量のコピーは実質的に不可能なので、この場

合には、ＨＤＤ２１へのコピーが許容される。そこで、ステップＳ４１に進み、利用条件管理プログラム１４０は、期限データベースの日時を、過去の登録日時から現在の日時（ＲＴＣ３５の出力する日時）に変更させる。そして、ステップＳ３８に戻り、利用条件管理プログラム１４０は、再び、期限データベース全体のハッシュ値をＣＰＵ３２に計算させ、不揮発性メモリ３４に保存させるとともに、ステップＳ３９において、そのコンテンツに対して未登録のフラグを設定する。

一方、ステップＳ４０において、現在時刻が登録日時より、まだ４８時間以上経過していないと判定された場合、その選択されたコンテンツのＨＤＤ２１へのコピーが禁止される。そこで、この場合には、ステップＳ４２に進み、利用条件管理プログラム１４０は、その選択されたコンテンツに対応して登録済みのフラグを設定する。

ステップＳ４０の処理により、所定の時間が経過しなければ、コンテンツの新たなコピーを生成できないので、不正でない通常の使用を目的としたコンテンツのコピーの生成を不当に妨げることなく、例えば、不正な販売又は配布などに必要な大量のコンテンツのコピーの生成は、実質的に不可能となる。なお、ステップＳ４０においては、判定の基準は４８時間以上の経過としたが、４８時間に限らず、例えば、１２時間乃至１６８時間のいずれかの時間であればよい。

以上のようにして、期限データベースチェック処理により、選択されたコンテンツがＨＤＤ２１に登録されているか否かを表すフラグが設定される。

図７に戻り、ステップＳ１３においてコピー管理プログラム１３

３は、選択されたコンテンツが期限データベースに登録済みであるか否かを、上述したフラグから判定する。選択されたコンテンツが登録済みである場合には、ステップＳ１４に進み、コピー管理プログラム１３３は、録音プログラム１１３に、例えば、「この曲は一度コピーされてからまだ４８時間以上経過していないので、コピーすることができません」のようなメッセージをディスプレイ２０に表示させる。これにより、使用者は、そのコンテンツをＨＤＤ２１にコピーすることができない理由を知ることができる。

ステップＳ１３において、選択したコンテンツが期限データベースに登録されていないと判定された場合、ステップＳ１５に進み、録音プログラム１１３は、ドライブ２２を制御し、そこに装着されているＣＤからコンテンツを読み出させる。このコンテンツには、図１０に示すように、所定の位置にウォータマークコードが挿入されている。録音プログラム１１３は、ステップＳ１６において、コンテンツに含まれているウォータマークコードを抽出し、そのウォータマークコードがコピー禁止を表しているいるか否かをステップＳ１７において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップＳ１８に進み、録音プログラム１１３は、録音プログラム１１３に例えば、「コピーは禁止されています」のようなメッセージをインターフェース１７を介してディスプレイ２０に表示させ、コピー処理を終了させる。

これに対して、ステップＳ１７において、ウォータマークがコピー禁止を表していないと判定された場合、ステップＳ１９に進み、録音プログラム１１３は、コンテンツを、圧縮／伸張プログラム１３８に、例えば、ＡＴＲＡＣ(Adaptive Transform Acoustic Codin

g)3（商標）などの方式で、ソフトウェア処理により圧縮させる。ステップＳ２０において、録音プログラム１１３は、暗号化プログラム１３７に、予め設定され、メモリ１３に記憶されている暗号鍵を用いて、例えば、ＤＥＳ(Data Encryption Standard)方式、ＦＥＡＬ(Fast Encripherment Algotithm)方式などの暗号化方法により、コンテンツを暗号化させる。暗号鍵は、この他、例えば、ソフトウェアにより発生した乱数、あるいはアダプタ２６のＣＰＵ３２により発生させた乱数に基づいて生成したものを用いることもできる。このように、パーソナルコンピュータ１だけではなく、それに付随して装着されたハードウェアとしてのアダプタ２６のＣＰＵ３２と、共働して暗号化処理を実行するようにすることで、解読がより困難となる暗号化を行うことが可能となる。

次に、ステップＳ２１において、録音プログラム１１３は、暗号化されたデータを、コンテンツデータベース１１４に転送し、１つのファイル（コンテンツファイル１６１として）としてファイル名を付けてＨＤＤ２１に保存させる。あるいはまた、１つのファイルの一部として、そのファイル名の位置情報（例えば、先頭からのバイト数）を与えて保存するようにしてもよい。

この保存処理と、上記した圧縮符号化処理及び暗号化処理とは別々に行うようにしてもよいし、同時に平行的に行うようにしてもよい。

さらに、ステップＳ２２において、録音プログラム１１３は、暗号化プログラム１３７に、予め定められている不揮発性メモリ３４に記憶されている保存用鍵を使って、上述したＤＥＳ方式、ＦＥＡＬ方式などの方式で、コンテンツを暗号化した暗号鍵を暗号化させ、

ＨＤＤ２１の曲データベース（図４に示すコンテンツデータベース１１４の利用条件ファイル１６２－１乃至１６２－Ｎに対応する）に保存する。

ステップＳ２３において、録音プログラム１１３は、保存したファイルに関する情報、暗号化された暗号鍵、そのコンテンツの情報、使用者がＧＵＩを介して入力した曲名の情報の要素を組にしてＨＤＤ２１の曲データベースに登録する（利用条件ファイル１６２－１乃至１６２－Ｎとして記録する）。そして、ステップＳ２４において、録音プログラム１１３は、ＣＰＵ３２に、曲データベース全体のハッシュ値を計算させ、不揮発性メモリ３４に保存させる。

このようにして、例えば、図１１に示すような曲データベースが、ＨＤＤ２１上に登録される。この例においては、アイテム１乃至アイテム３のファイル名、暗号化された暗号鍵、曲名、長さ、再生条件（開始日時、終了日時、回数制限）、再生回数カウンタ、再生時課金条件、コピー条件（回数）、コピー回数カウンタ及びコピー条件（ＳＣＭＳ）が記録されている。

例えば、ＳＤＭＩ(Secure Digital Music Initiative) が規定する方式では、ＣＤからコピーしたコンテンツに対応して、そのコンテンツがチェックアウトできる回数は、３回に設定される。

ＣＤからＨＤＤ２１にコンテンツが複製されて一定期間が経過すると、再びコンテンツを複製することができるようにしたので、ユーザの個人の使用の範囲とされる、数回の複製が可能となる。一方、個人の使用の範囲を超えて、例えば、大量に複製しようとすると、莫大な時間が必要とされ、現実的に不可能になる。また、例えば、パーソナルコンピュータ１が故障して、ＨＤＤ２１に記録されてい

たコンテンツが消去された場合においても、一定期間の経過後、消去されたコンテンツを再び複製し、ＨＤＤ２１に記録することができる。

また、例えば、ネットワーク２を介してＨＤＤ２１に記録されている期限データベースの内容を共有することもできる。

以上においては、ＩＳＲＣに対応して複製された日時が記憶されている場合を例として説明したが、コンテンツやＣＤを識別する情報であれば、他のもの（例えば、曲名、アルバム名、それらの組合せなど）を利用することもできる。

次に、図１２乃至図１４のフローチャートを参照して、表示操作指示プログラム１１２及びコンテンツ管理プログラム１１１を実行するＣＰＵ１１及びメインプログラムを実行するＣＰＵ５２による、ＨＤＤ２１からポータブルデバイス６のフラッシュメモリ６１（例えば、メモリースティック（商標））に、コンテンツを移動する処理及びチェックアウトの処理について説明する。

始めに、コンテンツの移動の処理について説明する。ステップＳ５１において、移動管理プログラム１３４は、利用条件管理プログラム１４０に、曲データベース全体のハッシュ値を計算させ、ステップＳ５２で、前回ＣＰＵ３２に計算させ、不揮発性メモリ３４に保存しておいたハッシュ値と比較する。両者が一致しない場合、移動管理プログラム１３４は、ステップＳ５３に進み、表示操作指示プログラム１１２に、例えば、「曲データベースが改竄された恐れがあります」のようなメッセージをディスプレイ２０に表示させた後、処理を終了させる。この場合の処理は、図８のステップＳ３１乃至ステップＳ３４の処理と同様の処理である。この場合において

は、ＨＤＤ２１からポータブルデバイス６へのコンテンツの移動が実行されないことになる。

次に、ステップＳ５４において、移動管理プログラム１３４は、ＨＤＤ２１に形成されている曲データベース（コンテンツデータベース１１４に含まれる）から、そこに登録されているコンテンツの情報を読み出し、表示操作指示プログラム１１２に、選択のためのＧＵＩとしてディスプレイ２０に表示させる。使用者は、この選択のためのＧＵＩに基づいて、ＨＤＤ２１からポータブルデバイス６へ移動させるコンテンツを、図５のフィールド２１２に表示される曲名、ボタン２１６などをクリックして選択する。次に、ステップＳ５５において、移動管理プログラム１３４は、ステップＳ５４で選択された選択されたコンテンツの再生条件、コピー条件、再生時課金条件などを調べる。この処理の詳細は、図１５のフローチャートを参照して後述する。

次に、ステップＳ５６において、パーソナルコンピュータ１の認証プログラム１４１とポータブルデバイス６のＣＰＵ５３との間において、相互認証処理が行われ、通信用鍵が共有される。

例えば、ポータブルデバイス６のフラッシュメモリ６１（又は、ＥＥＰＲＯＭ６８）には、マスター鍵ＫＭが予め記憶されており、パーソナルコンピュータ１のＲＡＭ１３（又は、ＨＤＤ２１の所定のファイル）には、個別鍵ＫＰとＩＤが予め記憶されているものとする。ＣＰＵ５３は、認証プログラム１４１から、ＲＡＭ１３に予め記憶されているＩＤの供給を受け、そのＩＤと自分自身が有するマスター鍵ＫＭにハッシュ関数を適用して、ＲＡＭ１３に記憶されているパーソナルコンピュータ１の個別鍵と同一の鍵を生成する。

このようにすることで、パーソナルコンピュータ１とポータブルデバイス６の両方に、共通の個別鍵が共有されることになる。この個別鍵を用いてさらに、一時的な通信用鍵を生成することができる。

あるいはまた、パーソナルコンピュータ１のＲＡＭ１３にＩＤとマスター鍵ＫＭＰを予め記憶させておくとともに、ポータブルデバイス６のフラッシュメモリ６１にもポータブルデバイス６のＩＤとマスター鍵ＫＭＭを記憶させておく。そして、それぞれのＩＤとマスター鍵をお互いに他方に送信することで、他方は一方から送信されてきたＩＤとマスター鍵にハッシュ関数を適用して、他方の個別鍵を生成する。そして、その個別鍵から、一時的な通信用鍵をさらに生成するようにする。

なお、認証の方法としては、例えば、ＩＯＳ(International Organization for Standardization)９７９８－２を利用することができる。

相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、ステップＳ５７において、移動管理プログラム１３４は、コンテンツデータベース１１４に、選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツ（例えば、図７のステップＳ２０の処理で暗号化されている）をＨＤＤ２１から読み出す。ステップＳ５８において、移動管理プログラム１３４は、ステップＳ５７で読み出したデジタルデータであるコンテンツの圧縮符号化方式（ステップＳ１９の処理）、暗号化方式（ステップＳ２０の処理）、フォーマット（例えば、ヘッダの方式など）などをポータブルデバイス６のものに変換する処理を実行する。この変換処理の詳細は、図１７のフロ

ーチャートを参照して後述する。

ステップＳ５９において、移動管理プログラム１３４は、ＰＤ用ドライバ１４３に、ステップＳ５８で変換したコンテンツを、ＵＳＢポート２３を介してポータブルデバイス６に転送させる。ステップＳ６０において、ポータブルデバイス６のＣＰＵ５３は、ＵＳＢコネクタ５６を介してこの伝送されてきたコンテンツを受信すると、そのコンテンツを、そのままフラッシュメモリ６１に記憶させる。

ステップＳ６１において、移動管理プログラム１３４は、さらに、利用条件変換プログラム１３９に、曲データベースに登録されているその選択されたコンテンツの再生条件（開始日時、終了日時、回数制限など）を、ポータブルデバイス６が管理している形式に変換する。ステップＳ６２において、移動管理プログラム１３４は、さらに、利用条件変換プログラム１３９に、選択されたコンテンツの曲データベース中に登録されているコピー条件中のＳＣＭＳ情報を、ポータブルデバイス６の管理する形式に変換させる。そして、ステップＳ６３において、移動管理プログラム１３４は、ＰＤ用ドライバ１４３に、ステップＳ６１で変換した再生条件と、ステップＳ６２で変換したＳＣＭＳ情報を、ポータブルデバイス６に転送させる。ポータブルデバイス６のＣＰＵ５３は、転送を受けた再生条件とＳＣＭＳ情報を、フラッシュメモリ６１に保存する。

ステップＳ６４において、移動管理プログラム１３４はまた、ＰＤ用ドライバ１４３に、選択されたコンテンツの曲データベース中に登録されている再生条件、再生時課金条件、コピー条件などを、ＣＰＵ１１が曲データベース中で扱っている形式のまま、ポータブルデバイス６に転送させ、フラッシュメモリ６１に保存させる。

ステップＳ６５において、移動管理プログラム１３４は、コンテンツデータベース１１４に、選択されたコンテンツの暗号化されている暗号鍵を曲データベースから読み出させ、ステップＳ６６において、復号プログラム１４２に、その暗号鍵をＲＡＭ１３に保存されている保存用鍵で復号させ、暗号化プログラム１３７に通信用鍵で暗号化させる。そして、通信用鍵で暗号化した暗号鍵を、移動管理プログラム１３４は、ＰＤ用ドライバ１４３に、ポータブルデバイス６へ転送させる。

ポータブルデバイス６のＣＰＵ５３は、ステップＳ６７で、パーソナルコンピュータ１から転送されてきた暗号鍵を相互認証処理で共有した通信用鍵を用いて復号し、自分自身の保存用鍵を用いて暗号化し、既に保存したデータと関連付けて、フラッシュメモリ６１に保存する。

ＣＰＵ５３は、暗号鍵の保存が完了すると、ステップＳ６８において、パーソナルコンピュータ１に対して暗号鍵を保存したことを通知する。パーソナルコンピュータ１の移動管理プログラム１３４は、ポータブルデバイス６からこの通知を受けると、ステップＳ６９において、コンテンツデータベース１１４に、そのコンテンツに対応するコンテンツファイル１６１を削除させるとともに、曲データベースからそのコンテンツの要素の組（すなわち、利用条件ファイル１６２）を削除させる。すなわち、これにより、コピーではなく、移動（ムーブ）が行われることになる。そして、ステップＳ７０において、移動管理プログラム１３４は、アダプタ２６のＣＰＵ３２に、曲データベースのデータを転送し、全体のハッシュ値を計算させ、不揮発性メモリ３４に保存させる。このハッシュ値が、上

述したステップＳ５２において、前回保存しておいたハッシュ値として用いられることになる。

次に、パーソナルコンピュータ１からポータブルデバイス６にコンテンツをチェックアウトする処理について説明する。パーソナルコンピュータ１からポータブルデバイス６にコンテンツをチェックアウトする処理は、図１２乃至図１４のパーソナルコンピュータ１からポータブルデバイス６へコンテンツを移動させる場合と同様の処理である。すなわち、チェックアウトの処理は、パーソナルコンピュータ１においてチェックイン／チェックアウト管理プログラム１３２により実行され、図１４のステップＳ６９において、コンテンツを削除する処理に代えて、曲データベースに記録されている、チェックアウトされたコンテンツのチェックアウトした回数（又はチェックアウトできる回数）を更新する処理を実行することを除いて、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

次に、コンテンツ管理プログラム１１１を実行するＣＰＵ１１による、図１２のステップＳ５５における選択されたコンテンツの再生条件などのチェック処理について図１５のフローチャートを参照して説明する。ステップＳ８１において、移動管理プログラム１３４は、コンテンツデータベース１１４に、曲データベースから、各種の条件を読み出させる。移動管理プログラム１３４は、ステップＳ８２において、ステップＳ８１で読み出した各種条件のうち、コピー回数がコピー制限回数を既に過ぎているか否かを判定する。コピー回数が、コピー制限回数を既にすぎている場合には、それ以上コピーを許容する訳にはいかないので、ステップＳ８３に進み、移

動管理プログラム１３４は、表示操作指示プログラム１１２に、例えば、「既にコピー回数がコピー制限回数に達しています」のようなメッセージをディスプレイ２０に表示させ、処理を終了させる。ステップＳ８２において、コピー回数がコピー制限回数を過ぎていないと判定された場合、ステップＳ８４に進み、現在日時が再生終了日時を過ぎているか否かの判定が行われる。現在日時としては、アダプタ２６のＲＴＣ３５より出力されたものが用いられる。これにより、使用者が、パーソナルコンピュータ１の現在時刻を意図的に過去の値に修正したものが用いられるようなことが防止される。移動管理プログラム１３４は、この現在日時をＣＰＵ３２から提供を受けて、ステップＳ８４の判断を自ら行うか、又は、ステップＳ８１で、曲データベースから読み出した再生条件をアダプタ２６のＣＰＵ３２に供給し、ＣＰＵ３２に、ステップＳ８４の判定処理を実行させる。

現在日時が再生終了日時を過ぎている場合、ステップＳ８５に進み、移動管理プログラム１３４は、コンテンツデータベース１１４に、選択されたコンテンツをＨＤＤ２１から消去させるとともに、曲データベースから、その選択されたコンテンツの情報を消去させる。ステップＳ８６において、移動管理プログラム１３４は、ＣＰＵ３２に、曲データベースのハッシュ値を計算させ、それを不揮発性メモリ３４に保存させる。以後、処理は終了される。したがって、この場合、コンテンツの移動が実行されない。

ステップＳ８４において、現在日時が、再生終了日時を過ぎていないと判定された場合、ステップＳ８７に進み、移動管理プログラム１３４は、その選択されたコンテンツの再生時課金条件（例えば、

再生１回当たりの料金）が曲データベース中に登録されているか否かを判定する。再生時課金条件が登録されている場合には、移動管理プログラム１３４は、ステップＳ８８において、ＰＤ用ドライバ１４３に、ポータブルデバイス６と通信させ、ポータブルデバイス６に課金機能が存在するか否かを判定する。ポータブルデバイス６に課金機能が存在しない場合には、選択されたコンテンツをポータブルデバイス６に転送する訳にはいかないので、ステップＳ８９において、移動管理プログラム１３４は、表示操作指示プログラム１１２に、例えば、「転送先が課金機能を有しておりません」のようなメッセージをディスプレイ２０に表示させ、コンテンツの移動処理を終了させる。

ステップＳ８７において再生時課金条件が登録されていないと判定された場合、又は、ステップＳ８８において、ポータブルデバイス６に課金機能が存在すると判定された場合、ステップＳ９０に進み、移動管理プログラム１３４は、選択されたコンテンツに関し、例えば、再生制限回数などのその他の再生条件が登録されているか否かを判定する。その他の再生条件が登録されている場合には、ステップＳ９１に進み、移動管理プログラム１３４は、ポータブルデバイス６に、その再生条件を守る機能が存在するか否かを判定する。ポータブルデバイス６が、その再生条件を守る機能を有していない場合には、ステップＳ９２に進み、移動管理プログラム１３４は、表示操作指示プログラム１１２に、例えば、「転送先の装置が再生条件を守る機能を有しておりません」のようなメッセージをディスプレイ２０に表示させ、処理を終了させる。

ステップＳ９０において、再生条件が登録されていないと判定さ

れた場合、又はステップＳ９１において、ポータブルデバイス６が再生条件を守る機能を有していると判定された場合、再生条件等のチェック処理が終了され、図１２のステップＳ５６に戻る。

図１６は、ポータブルデバイス６が管理している（守ることが可能な）再生条件の例を表している。図１６に示す再生情報は、例えば、ＥＥＰＲＯＭ６８に記憶されている。この例においては、アイテム１乃至アイテム３の各コンテンツについて、再生開始日時と再生終了日時が登録されているが、再生回数は、アイテム２についてのみ登録されており、アイテム１とアイテム３については登録されていない。したがって、アイテム２のコンテンツが選択されたコンテンツとされた場合、再生回数の再生条件は守ることが可能であるが、アイテム１又はアイテム３のコンテンツが選択されたコンテンツとされた場合、再生回数の条件は守ることができないことになる。

次に、図１７のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するＣＰＵ１１による、図１２のステップＳ５８におけるフォーマット変換処理の詳細について説明する。ステップＳ１０１において、移動管理プログラム１３４は、コンテンツデータベース１１４に記録されている選択されたコンテンツのフォーマット（例えば、再生条件、使用条件、コピー条件などを含むヘッダなどの方式）を調べる。ステップＳ１０２において、移動管理プログラム１３４は、相手先の機器（今の場合、ポータブルデバイス６）に設定することが可能な条件を調べる。すなわち、移動管理プログラム１３４は、ポータブルデバイス６のＣＰＵ５３に設定可能な条件を問い合わせ、その回答を得る。ステップＳ１０３において移動管理プログラム１３４は、曲データベース中に登録されている

フォーマットの条件のうち、相手先の機器に設定可能な条件をステップＳ１０２で調べた条件に基づいて決定する。

ステップＳ１０４において、移動管理プログラム１３４は、設定可能な条件が存在するか否かを判定し、設定可能な条件が存在しない場合には、ステップＳ１０５に進み、コンテンツをポータブルデバイス６に移動する処理を禁止する。すなわち、この場合には、曲データベース中に登録されている条件をポータブルデバイス６が守ることができないので、そのようなポータブルデバイス６には、コンテンツを移動することが禁止されるのである。

ステップＳ１０４において設定可能な条件が存在すると判定された場合、ステップＳ１０６に進み、移動管理プログラム１３４は、利用条件変換プログラム１３９に、その条件を相手先の機能フォーマットの条件（例えば、ポータブルデバイス６に転送する際、ヘッダに格納される条件）に変換させる。そして、ステップＳ１０７において、移動管理プログラム１３４は、変換した条件を相手先の機器に設定する。その結果、ポータブルデバイス６は、設定された条件に従って（その条件を守って）、コンテンツを再生することが可能となる。

次に、図１８乃至図２０のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するＣＰＵ１１及びメインプログラムを実行するＣＰＵ５３による、ＨＤＤ２１からポータブルデバイス６にコンテンツをコピーする場合の処理について説明する。この図１８乃至図２０のステップＳ１１１乃至ステップＳ１２７の処理は、コピー管理プログラム１３３により実行され、図１２乃至図１４のＨＤＤ２１からポータブルデバイス６へコンテンツを移動させ

る場合のステップＳ５１乃至ステップＳ６７の処理と同様の処理である。すなわち、この場合においても、曲データベースの改竄がチェックされた後、選択されたコンテンツの再生条件とのチェック処理が行われる。さらに、ポータブルデバイス６と、パーソナルコンピュータ１との間の相互認証処理の後、コンテンツが、パーソナルコンピュータ１のＨＤＤ２１からポータブルデバイス６のフラッシュメモリ６１に転送され、保存される。その後、ステップＳ１２８において、コピー管理プログラム１３３は、曲データベースのコピー回数カウンタを１だけインクリメントする。そして、ステップＳ１２９において、コピー管理プログラム１３３は、ＣＰＵ３２に、曲データベース全体のハッシュ値を計算させ、その値を不揮発性メモリ３４に保存させる。

次に、図２１のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するＣＰＵ１１及びメインプログラムを実行するＣＰＵ５３による、ポータブルデバイス６からＨＤＤ２１にコンテンツを移動する処理及びチェックインの処理について説明する。

始めに、コンテンツの移動の処理について説明する。ステップＳ１６１において、移動管理プログラム１３４は、ポータブルデバイス６のＣＰＵ５３に対してフラッシュメモリ６１に記憶されているコンテンツの情報の読み出しを要求する。ＣＰＵ５３は、この要求に対応して、フラッシュメモリ６１に記憶されているコンテンツの情報をパーソナルコンピュータ１に送信する。移動管理プログラム１３４は、この情報に基づいて、ディスプレイ２０に、フラッシュメモリ６１に記憶されているコンテンツを選択するためのＧＵＩを表示させる。使用者は、キーボード１８又はマウス１９を操作して、

そのＧＵＩに基づいて、ポータブルデバイス６からＨＤＤ２１（コンテンツデータベース１１４）に移動させるコンテンツを指定する。

ステップＳ１６２において、移動管理プログラム１３４は、認証プログラム１４１に、ＣＰＵ５３との間において、相互認証処理を実行させ、通信用鍵を共有させる。この処理は、図１２のステップＳ５６における場合と同様の処理である。

次に、ステップＳ１６３において、ＣＰＵ５３は、フラッシュメモリ６１に記憶されている暗号化されている選択されたコンテンツを読み出し、パーソナルコンピュータ１に転送する。移動管理プログラム１３４は、ステップＳ１６４において、ポータブルデバイス６から転送されてきたコンテンツを、１つのファイルとしてファイル名を付けて、コンテンツデータベース１１４（ＨＤＤ２１）に保存する。この保存は、例えば、１つのファイルの一部として、ファイル名の位置情報（例えば、先頭からのバイト数）を与えて行うようにすることもできる。

ステップＳ１６５において、ＣＰＵ５３は、フラッシュメモリ６１に記憶されている選択されたコンテンツの暗号化されている暗号鍵を読み出し、それを自分自身の保存用鍵で復号し、さらに通信用鍵で暗号化した後、パーソナルコンピュータ１に転送する。この暗号鍵は、例えば、図１４のステップＳ６７の処理でフラッシュメモリ６１に保存されていたものである。

ステップＳ１６６において、移動管理プログラム１３４は、ポータブルデバイス６から暗号鍵の転送を受けると、復号プログラム１４２に、それを通信用鍵で復号させ、暗号化プログラム１３７に、自分自身の保存用鍵で暗号化させる。ステップＳ１６７で、移動管

理プログラム１３４は、コンテンツデータベース１１４に、ステップＳ１６４で保存したコンテンツのファイル名、そのコンテンツの情報、使用者がＧＵＩを介して入力した曲名、ステップＳ１６６で暗号化した暗号鍵などを、ＨＤＤ２１の曲データベースに登録させる。そして、ステップＳ１６８において、移動管理プログラム１３４は、利用条件管理プログラム１４０に、その曲データベース全体のハッシュ値をＣＰＵ３２に計算させ、不揮発性メモリ３４に保存させる。

ステップＳ１６９において、移動管理プログラム１３４は、ポータブルデバイス６に対して暗号鍵が保存されたことを通知し、そのコンテンツの削除を要求する。ＣＰＵ５３は、パーソナルコンピュータ１から、そのコンテンツの削除が要求されてきたとき、ステップＳ１７０において、フラッシュメモリ６１に記憶されているそのコンテンツを削除する。

次に、ポータブルデバイス６からパーソナルコンピュータ１にコンテンツをチェックインする処理について説明する。ポータブルデバイス６からパーソナルコンピュータ１にコンテンツをチェックインする処理は、図２１のポータブルデバイス６からパーソナルコンピュータ１へコンテンツを移動させる場合と同様の処理である。すなわち、チェックインの処理は、パーソナルコンピュータ１においてチェックイン／チェックアウト管理プログラム１３２により実行され、図２１のステップＳ１６２乃至Ｓ１６６の処理が省略される。また、パーソナルコンピュータ１は、図２１のステップＳ１６７において、曲データベースに記録されている、チェックインされたコンテンツのチェックアウトできる回数を更新する処理を実行して、

ステップＳ１７０の処理の後、コンテンツファイルの削除を確認することを除いて、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

なお、ポータブルデバイス６のフラッシュメモリ６１がメモリカードとして着脱可能であるとき、パーソナルコンピュータ１は、チェックインの処理において、図２１のステップＳ１６２の相互認証の処理を実行する。

次に、コンテンツ管理プログラム１１１を実行するＣＰＵ１１及びメインプログラムを実行するＣＰＵ５３による、ポータブルデバイス６からＨＤＤ２１へコンテンツをコピーする場合の処理について、図２２のフローチャートを参照して説明する。この図２２に示すステップＳ１８１乃至ステップＳ１８８の処理は、図２１のポータブルデバイス６からＨＤＤ２１へコンテンツを移動させる場合の処理におけるステップＳ１６１乃至ステップＳ１６８の処理と同様の処理である。すなわち、コピー処理の場合は、コピー管理プログラム１３３により実行され、図２１のステップＳ１６９，Ｓ１７０の処理が省略される点を除いて、移動の場合の処理と基本的に同様の処理となるので、その説明は省略する。

次に、図２３のフローチャートを参照して、ＥＭＤサーバ４及びコンテンツ管理プログラム１１１を実行するＣＰＵ１１による、ＥＭＤサーバ４から転送を受けたコンテンツをＨＤＤ２１にコピーする処理について説明する。ステップＳ２０１において、購入用プログラム１４４は、図５に示すボタン２０２がクリックされて、使用者からＥＭＤサーバ４へのアクセスが指令されたとき、通信部２５を制御し、ネットワーク２を介してＥＭＤサーバ４にアクセスさせ

る。ＥＭＤサーバ４は、このアクセスに対応して、自分自身が保持しているコンテンツの曲番号、曲名、各情報などの情報を、ネットワーク２を介してパーソナルコンピュータ１に転送する。購入用プログラム１４４は、通信部２５を介して、この情報を取得したとき、表示操作指示プログラム１１２に、それをインターフェース１７を介してディスプレイ２０に表示させる。使用者は、ディスプレイ２０に表示されたＧＵＩを利用して、ステップＳ２０２において、コピーを希望するコンテンツを指定する。この指定情報は、ネットワーク２を介してＥＭＤサーバ４に転送される。ステップＳ２０３において、購入用プログラム１４４は、ＥＭＤサーバ４との間において、ネットワーク２を介して相互認証処理を実行し、通信用鍵を共有する。

パーソナルコンピュータ１とＥＭＤサーバ４との間で行われる相互認証処理は、例えば、ＩＳＯ　９７９８－３で規定される公開鍵と秘密鍵を用いて行うようにすることができる。この場合、パーソナルコンピュータ１は、自分自身の秘密鍵とＥＭＤサーバ４の公開鍵を予め有しており、ＥＭＤサーバ４は、自分自身の秘密鍵を有し、相互認証処理が行われる。パーソナルコンピュータ１の公開鍵は、ＥＭＤサーバ４から転送したり、あるいはパーソナルコンピュータ１に予め配布されている証明書(certificate) をパーソナルコンピュータ１からＥＭＤサーバ４に転送し、その証明書をＥＭＤサーバ４が確認し、公開鍵を得るようにしてもよい。さらに、ステップＳ２０４において、購入用プログラム１４４は、ＥＭＤサーバ４との間において課金に関する処理を実行する。この課金の処理の詳細は、図２４のフローチャートを参照して後述する。

次に、ステップＳ２０５において、ＥＭＤサーバ４は、パーソナルコンピュータ１に対して、ステップＳ２０２で指定された、暗号化されているコンテンツをネットワーク２を介してパーソナルコンピュータ１に転送する。このとき、時刻情報も適宜転送される。ステップＳ２０６において、購入用プログラム１４４は、コンテンツデータベース１１４に、転送を受けたコンテンツにファイル名を付けてＨＤＤ２１に１つのコンテンツファイル１６１として保存させる。ステップＳ２０７において、ＥＭＤサーバ４は、さらに、そのコンテンツの暗号鍵をステップＳ２０３でパーソナルコンピュータ１と共有した通信用鍵を用いて暗号化し、パーソナルコンピュータ１へ転送する。

購入用プログラム１４４は、ステップＳ２０８において、復号プログラム１４２に、ＥＭＤサーバ４より転送を受けた暗号鍵を単独で、又はアダプタ２６のＣＰＵ３２と共同して通信用鍵を用いて復号させ、暗号化プログラム１３７に、復号して得られた暗号鍵を自分自身の保存用鍵で暗号化させる。ステップＳ２０９において、購入用プログラム１４４は、コンテンツデータベース１１４に、そのコンテンツのファイル名、コンテンツの情報、使用者が入力した曲名、暗号化された暗号鍵を組にして、ＨＤＤ２１の曲データベースに登録させる。さらに、ステップＳ２１０において、購入用プログラム１４４は、その曲データベース全体のハッシュ値をＣＰＵ３２に計算させ、不揮発性メモリ３４に保存させる。

なお、ステップＳ２０５においてＥＭＤサーバ４は、コンテンツとともに、時刻データをパーソナルコンピュータ１に送信する。この時刻データは、パーソナルコンピュータ１からアダプタ２６に転

送される。アダプタ２６のＣＰＵ３２は、パーソナルコンピュータ１より転送されてきた時刻データを受信すると、ステップＳ２１１において、ＲＴＣ３５の時刻を修正させる。このようにして、相互認証の結果、正しい装置と認識された外部の装置から得られた時刻情報に基づいて、アダプタ２６のＲＴＣ３５の時刻情報を修正するようにしたので、アダプタ２６を常に正しい時刻情報を保持することが可能となる。

次に、図２４のフローチャートを参照して、ＥＭＤサーバ４及びコンテンツ管理プログラム１１１を実行するＣＰＵ１１による、図２３のステップＳ２０４における課金に関する処理の詳細について説明する。ステップＳ２２１において、購入用プログラム１４４は、ステップＳ２０１でＥＭＤサーバ４から伝送されてきた価格情報の中から、ステップＳ２０２で指定された選択されたコンテンツの価格情報を読み取り、これをＨＤＤ２１上の課金ログに書き込む。図２５は、このような課金ログの例を表している。この例においては、使用者は、アイテム１乃至アイテム３を、ＥＭＤサーバ４からコピーしており、アイテム１とアイテム２の領域は５０円とされ、アイテム３の料金は６０円とされている。その時点における課金ログのハッシュ値も、ＣＰＵ３２により計算され、不揮発性メモリ３４に登録されている。

次に、ステップＳ２２２において、購入用プログラム１４４は、ステップＳ２２１で書き込んだ課金ログをＨＤＤ２１から読み出し、これをネットワーク２を介してＥＭＤサーバ４に転送する。ＥＭＤサーバ４は、ステップＳ２２３において、パーソナルコンピュータ１から転送を受けた課金ログに基づく課金計算処理を実行する。す

なわち、ＥＭＤサーバ４は、内蔵するデータベースに、パーソナルコンピュータ１の使用者から伝送されてきた課金ログを追加更新する。そして、ステップＳ２２４において、ＥＭＤサーバ４は、その課金ログについて直ちに決裁するか否かを判定し、直ちに決裁する場合には、ステップＳ２２５に進み、ＥＭＤサーバ４は、決裁に必要な商品名、金額などを決裁サーバ（図示せず）に転送する。そして、ステップＳ２２６において、決裁サーバは、パーソナルコンピュータ１の使用者に対する決裁処理を実行する。ステップＳ２２４において、決裁は直ちには行われないと判定された場合、ステップＳ２２５とＳ２２６の処理はスキップされる。すなわち、この処理は、例えば、月に１回など、定期的にその後実行される。

次に、図２６と図２７のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するＣＰＵ１１による、音声入出力インターフェース２４のＩＥＣ６０９５８端子２４ａから入力された、図示せぬＣＤプレーヤなどからの再生されたコンテンツを、ＨＤＤ２１にコピーする場合の処理について説明する。ステップＳ２４１において、使用者は、ＣＤプレーヤのＩＥＣ６０９５８出力端子を、パーソナルコンピュータ１の音声入出力インターフェース２４のＩＥＣ６０９５８端子２４ａに接続する。ステップＳ２４２において、使用者は、キーボード１８又はマウス１９を操作し、ＣＤプレーヤからコピーするコンテンツの曲名（又は、コンテンツに対応する番号）を入力する。そして、ステップＳ２４３において使用者は、ＣＤプレーヤのボタンを操作し、ＣＤプレーヤの再生を開始させる。ＣＤプレーヤとパーソナルコンピュータ１との間に制御信号を送受する線が接続されている場合には、パーソナルコンピュータ１のキ

ーボード１８又はマウス１９を介して再生開始指令を入力することで、ＣＤプレーヤにＣＤの再生を開始させることも可能である。

ＣＤプレーヤにおいて、ＣＤの再生が開始されると、ステップＳ２４４において、ＣＤプレーヤから出力されたコンテンツが、ＩＥＣ６０９５８端子２４ａを介してパーソナルコンピュータ１に転送されてくる。ステップＳ２４５において、コピー管理プログラム１３３は、ＩＥＣ６０９５８端子２４ａを介して入力されてくるデータから、ＳＣＭＳ(Serial Copy Management System) データを読み取る。このＳＣＭＳデータには、コピー禁止、コピー１回限り可能、コピーフリーなどのコピー情報が含まれている。そこで、ステップＳ２４６において、ＣＰＵ１１は、ＳＣＭＳデータがコピー禁止を表しているか否かを判定し、コピー禁止を表している場合には、ステップＳ２４７に進み、コピー管理プログラム１３３は、表示操作指示プログラム１１２に、例えば、「コピーが禁止されています」といったメッセージをディスプレイ２０に表示させ、コピー処理を終了する。すなわち、この場合には、ＨＤＤ２１へのコピーが禁止される。

コピー管理プログラム１３３は、ステップＳ２４６において、ステップＳ２４５で読み取ったＳＣＭＳ情報がコピー禁止を表していないと判定した場合、ステップＳ２４８に進み、ウォータマークコードを読み出し、そのウォータマークがコピー禁止を表しているか否かをステップＳ２４９において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップＳ２４７に進み、上述した場合と同様に、所定のメッセージが表示され、コピー処理が終了される。

ステップＳ２４９において、ウォータマークがコピー禁止を表していないと判定された場合、ステップＳ２５０に進み、期限データベースチェック処理が行われる。期限データベースチェックの結果、選択されたコンテンツが既に登録されていれば、ステップＳ２５１，Ｓ２５２の処理で、処理が終了される。この処理は、図７のステップＳ１３，Ｓ１４の処理と同様の処理である。

選択されたコンテンツがまだＨＤＤ２１に登録されていないコンテンツであれば、ステップＳ２５３乃至Ｓ２５８で、その登録処理が実行される。このステップＳ２５３乃至ステップＳ２５８の処理は、ステップＳ２５７において、ＩＥＣ６０９５８端子２４ａから供給されてくるＳＣＭＳ情報も曲データベースに登録される点を除き、図７のステップＳ１９乃至ステップＳ２４の処理と同様の処理であるので、その説明は省略する。

次に、図２８と図２９のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するＣＰＵ１１による、コンテンツをＨＤＤ２１からＩＥＣ６０９５８端子２４ａに出力（再生）する場合の処理について説明する。ステップＳ２７１乃至ステップＳ２７３において、図１８のステップＳ１１１乃至Ｓ１１３における場合と同様に、曲データベース全体のハッシュ値が計算され、前回保存しておいたハッシュ値と一致するか否かが判定され、曲データベースの改竄のチェック処理が行われる。曲データベースの改竄が行われていないと判定された場合、ステップＳ２７４に進み、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、ＨＤＤ２１の曲データベースにアクセスさせ、そこに登録されている曲の情報を読み出させ、

ディスプレイ２０に表示させる。使用者は、その表示を見て、キーボード１８又はマウス１９を適宜操作して、再生出力するコンテンツを選択する。ステップＳ２７５において、表示操作指示プログラム１１２は、選択されたコンテンツの再生条件等のチェック処理を実行する。この再生条件等のチェック処理の詳細は、図３０のフローチャートを参照して後述する。

次に、ステップＳ２７６において、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、ステップＳ２７４において選択されたコンテンツの暗号鍵を曲データベースから読み出させ、復号プログラム１４２に保存用鍵で復号させる。ステップＳ２７７において、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、選択されたコンテンツのＳＣＭＳ情報を曲データベースから読み出させ、ＩＥＣ６０９５８端子２４ａから出力するＳＣＭＳ情報を、ＳＣＭＳシステムの規則に従って決定する。例えば、再生回数に制限があるような場合、再生回数は１だけインクリメントされ、新たなＳＣＭＳ情報とされる。ステップＳ２７８において、表示操作指示プログラム１１２はさらに、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、選択されたコンテンツのＩＳＲＣを曲データベースから読み出させる。

次に、ステップＳ２７９において、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、曲データベースから選択されたコンテンツファイル名を読み出させ、そのファイル名を基に、そのコンテンツをＨ

ＤＤ２１から読み出させる。表示操作指示プログラム１１２はさらに、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、そのコンテンツに対応する暗号鍵を曲データベースから読み出させ、復号プログラム１４２に、保存用鍵で復号させ、復号した暗号鍵を用いて、暗号化されているコンテンツを復号する。圧縮／伸張プログラム１３８は、さらに、そのコンテンツの圧縮符号を復号（伸張）する。ステップＳ２８０において、表示操作指示プログラム１１２は、ドライバ１１７に、ステップＳ２７９で、復号したデジタルデータであるコンテンツを、ステップＳ２７７で決定したＳＣＭＳ情報、並びにステップＳ２７８で読み出したＩＳＲＣ情報とともに、ＩＥＣ６０９５８の規定に従って、ＩＥＣ６０９５８端子２４ａから出力させる。さらにまた、表示操作指示プログラム１１２は、例えば、図示せぬリアルプレーヤ（商標）などのプログラムを動作させ、デジタルデータであるコンテンツをアナログ化させ、音声入出力インターフェース２４のアナログ出力端子から出力させる。

ステップＳ２８１において、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、曲データベース中の再生回数カウンタの値を１だけインクリメントさせる。そして、ステップＳ２８２において、選択されたコンテンツに再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップＳ２８３に進み、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、対応する料金を課金ログに書き込ませ、ステップＳ２８４において、表示操

作指示プログラム１１２は、利用条件管理プログラム１４０に、曲データベース全体のハッシュ値をＣＰＵ３２に計算させ、不揮発性メモリ３４に記憶させる。ステップＳ２８２において、選択されたコンテンツに再生時課金条件が付加されていないと判定された場合、ステップＳ２８３とステップＳ２８４の処理はスキップされる。

次に、図３０のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するＣＰＵ１１による、図２８のステップＳ２７５の再生条件等のチェック処理の詳細について説明する。ステップＳ３０１において、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、曲データベースの各種条件を読み出させる。ステップＳ３０２において利用条件管理プログラム１４０は、読み出した条件のうち、再生回数が制限回数を過ぎているか否かを判定し、過ぎている場合には、ステップＳ３０３に進み、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、選択されたコンテンツをＨＤＤ２１から削除させるとともに、曲データベースから選択されたコンテンツの情報を削除させる。ステップＳ３０４において、表示操作指示プログラム１１２はさらに、利用条件管理プログラム１４０に、曲データベースの新たなハッシュ値をＣＰＵ３２に計算させ、そのハッシュ値を不揮発性メモリ３４に保存させる。この場合、再生出力は禁止される。

ステップＳ３０２において、再生回数が制限回数を過ぎていないと判定された場合、ステップＳ３０５に進み、利用条件管理プログラム１４０２は、再生終了日時が現在日時を過ぎているか否かを判定する。再生終了日時が現在日時を過ぎている場合には、上述した

場合と同様にステップＳ３０３において、選択されたコンテンツをＨＤＤ２１から削除させるとともに、曲データベースからも削除させる。そして、ステップＳ３０４において、新たな曲データベースのハッシュ値が計算され、保存される。この場合にも、再生出力は禁止される。

ステップＳ３０５において、再生終了日時が現在日時を過ぎていないと判定された場合は、ステップＳ３０６に進み、ＣＰＵ３２は、その選択されたコンテンツに対して再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップＳ３０７に進み、表示操作指示プログラム１１２は、再生時課金条件が付加されている旨のメッセージと料金を、ディスプレイ２０に表示させる。ステップＳ３０６において、再生時課金条件が付加されていないと判定された場合、ステップＳ３０７の処理はスキップされる。

次に、図３１と図３２のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するＣＰＵ１１及びメインプログラムを実行するＣＰＵ５３による、ＨＤＤ２１からポータブルデバイス６経由でコンテンツを出力（再生）する場合の処理について説明する。ステップＳ３２１乃至ステップＳ３２５において、曲データベースの改竄チェックと選択されたコンテンツの指定、並びに選択されたコンテンツの再生条件等のチェック処理が行われる。その処理は、図２８のステップＳ２７１乃至ステップＳ２７５の処理と同様の処理であるので、その説明は省略する。

ステップＳ３２６において、ポータブルデバイス６とパーソナルコンピュータ１の間で相互認証処理が実行され、相互の間で、通信

用鍵が共有される。ステップＳ３２７において、表示操作指示プログラム１１２は、ポータブルデバイス６に対して、これから送る暗号化されているコンテンツを再生するように命令する。ステップＳ３２８において、表示操作指示プログラム１１２は、ステップＳ３２４で、コンテンツ管理プログラム１１１を介してコンテンツデータベース１１４に、指定された選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツをＨＤＤ２１から読み出させる。表示操作指示プログラム１１２は、ステップＳ３２９において、コンテンツ管理プログラム１１１に、コンテンツの圧縮符号化方式、暗号化方式、フォーマットなどをポータブルデバイス６の方式のものに変換する処理を実行させる。そして、ステップＳ３３０において、表示操作指示プログラム１１２は、暗号化プログラム１３７に、ステップＳ３２９において変換したコンテンツを通信用鍵で暗号化させ、ポータブルデバイス６に転送する。

ステップＳ３３１において、ポータブルデバイス６のＣＰＵ５３は、ステップＳ３２７において、パーソナルコンピュータ１から転送されてきた命令に対応して、転送を受けた各データを通信用鍵で復号し、再生出力する。ステップＳ３３２において、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介してコンテンツデータベース１１４に、曲データベースの再生回数カウントを１だけインクリメントさせる。さらに、ステップＳ３３３において、表示操作指示プログラム１１２は、選択されたコンテンツに再生時課金条件が付加されているか否かを判定し、付加されている場合には、ステップＳ３３４において、コンテンツ管理プログラム

１１１を介してコンテンツデータベース１１４に、その料金を課金ログに書き込ませ、ステップＳ３３５において、ＣＰＵ３２に、曲データベース全体のハッシュ値を新たに計算させ、保存させる。選択されたコンテンツに再生時課金条件が付加されていない場合には、ステップＳ３３４，ステップＳ３３５の処理はスキップされる。

本発明においては、コンテンツが不正に複製されるのを防止するために、各種の工夫が凝らされている。例えば、ＣＰＵ１１を動作させるプログラムは、その実行順序が毎回変化するような、いわゆるタンパーレジスタントソフトウェアとされている。

さらに、上述したように、ＣＰＵ１１の機能の一部は、ハードウェアとしてのアダプタ２６に分担され、両者が共働して各種の処理を実行するようになされている。これにより、より安全性を高めることが可能となっている。

例えば、上述したように、曲データベースのハッシュ値は、曲データベース自体に保存されるのではなく、アダプタ２６の不揮発性メモリ３４に保存される。すなわち、図８のステップＳ３２，Ｓ３３などの前回保存しておいたハッシュ値との比較処理において、比較対象とされる過去のハッシュ値は、不揮発性メモリ３４に記憶されているものとされる。これにより、例えば、他の記録媒体にコピー又は移動させる前に、ＨＤＤ２１に保存されているコンテンツを含む記録内容の全てをバックアップしておき、ＨＤＤ２１から、そこに保存されているコンテンツを他の記録媒体にコピー又は移動した後、ＨＤＤ２１にバックアップしておいた記録内容に含まれるコンテンツを再びリストアするようにすることで、利用条件を無視して、実質的に際限なく、コピー又は移動ができてしまうようなこと

が防止される。

例えば、図３３に示すように、ＨＤＤ２１にコンテンツＡ，Ｂが保存されている場合、不揮発性メモリ３４には、コンテンツＡとコンテンツＢの情報に対応するハッシュ値が保存されている。この状態において、ＨＤＤ２１のコンテンツＡ，Ｂを含む記録データの一部又は全部を他の記録媒体２７１にバックアップしたとする。その後、ＨＤＤ２１に保存されているコンテンツＡとコンテンツＢのうち、コンテンツＡを他の記録媒体２７２に移動させた場合、その時点において、ＨＤＤ２１に記録されているコンテンツは、コンテンツＢだけとなるので、不揮発性メモリ３４のハッシュ値も、コンテンツＢに対応するハッシュ値に変更される。

したがって、その後、記録媒体２７１にバックアップしておいたＨＤＤ２１のコンテンツＡ，Ｂを含む記録データの一部又は全部をＨＤＤ２１にリストアして、ＨＤＤ２１に、再びコンテンツＡとコンテンツＢを保存させたとしても、不揮発性メモリ３４には、コンテンツＢの情報から演算されたハッシュ値が記憶されており、コンテンツＡとコンテンツＢの情報から演算されたハッシュ値は記憶されていない。これにより、その時点において、ＨＤＤ２１に記憶されているコンテンツＡとコンテンツＢに基づくハッシュ値が、不揮発性メモリ３４に記憶されている過去のハッシュ値と一致しないことになり、曲データベースが改竄されたことが検出される。その結果、以後、ＨＤＤ２１に保存されているコンテンツＡとコンテンツＢの利用が制限されてしまうことになる。

さらに、上述したように、アダプタ２６は、ＲＴＣ３５を内蔵しており、このＲＴＣ３５の値は、正しい認証結果が得られた他の装

置（例えば、ＥＭＤサーバ４）から転送されてきた時刻データに基づいて、その時刻情報を修正する。そして、現在日時としては、パーソナルコンピュータ１が管理するものではなく、ＲＴＣ３５が出力するものが利用される。したがって、使用者が、パーソナルコンピュータ１の現在時刻を故意に過去の時刻に修正し、再生条件としての再生終了日時の判定を免れるようなことができなくなる。

また、アダプタ２６は、暗号化されて転送されてきたプログラムをＲＯＭ３６に予め記憶されているプログラムに従って復号し、実行するように構成することで、より安全性が高められている。次に、この点について、図３４のフローチャートを参照して説明する。

すなわち、パーソナルコンピュータ１は、アダプタ２６に対して、所定の処理を実行させたいとき、ステップＳ３５１において、アダプタ２６に実行させるべきプログラムをＲＡＭ１３に予め記憶されている暗号鍵を用いて暗号化してアダプタ２６に転送する。アダプタ２６のＲＯＭ３６には、パーソナルコンピュータ１から転送されてきた、暗号化されているプログラムを復号し、実行するためのプログラムが予め記憶されている。ＣＰＵ３２は、このＲＯＭ３６に記憶されているプログラムに従って、パーソナルコンピュータ１から転送されてきた暗号化されているプログラムをステップＳ３５２において復号する。そして、ステップＳ３１３において、ＣＰＵ３２は、復号したプログラムをＲＡＭ３３に展開し、ステップＳ３５４において、そのプログラムを実行する。

例えば、上述したように、パーソナルコンピュータ１のＣＰＵ１１は、ＨＤＤ２１の曲データベースのハッシュ値をアダプタ２６に計算させるとき、曲データベースのデータを暗号鍵で暗号化してア

ダプタ２６のＣＰＵ３２に転送する。ＣＰＵ３２は、転送されてきた曲データベースのデータに対してハッシュ関数を適応し、ハッシュ値を計算する。そして、計算されたハッシュ値を不揮発性メモリ３４に記憶させる。あるいは、そのハッシュ値を、ＣＰＵ３２は、予め記憶されている過去のハッシュ値と比較し、比較結果をパーソナルコンピュータ１のＣＰＵ１１に転送する。

図３５は、アダプタ２６の内部のより具体的な構成を表している。アダプタ２６は、半導体ＩＣとして形成される。アダプタ２６は、図２に示したインターフェース３１、ＣＰＵ３２、ＲＡＭ３３、不揮発性メモリ３４、ＲＴＣ３５、ＲＯＭ３６以外に、ＲＡＭ３３に対する書き込みと読み出しを制御するＲＡＭコントローラ３０１、並びに論理回路３０２を有している。論理回路３０２は、例えば、暗号化されているコンテンツを解読した後、解読したデータをアダプタ２６から直接出力するような場合の処理のために用いられる。

これらのインターフェース３１乃至ＲＯＭ３６、ＲＡＭコントローラ３０１並びに論理回路３０２は、半導体ＩＣ内に一体的に組み込まれ、外部からは分解できないように構成されている。

水晶振動子３１１は、アダプタ２６が各種の処理を実行する上において、基準となるクロックを生成するとき用いられる。発振回路３１２は、ＲＴＣ３５を動作させるための発振回路である。バッテリ３１３は、発振回路３１２、不揮発性メモリ３４及びＲＴＣ３５に対してバックアップ用の電力を供給している。アダプタ２６のその他の回路には、パーソナルコンピュータ１の電源供給回路３２１からの電力が供給されている。

不揮発性メモリ３４は、書き込み消去可能なＲＯＭで構成するこ

とも可能であるが、バッテリ３１３からのバックアップ電源でバックアップされるＲＡＭで構成する場合には、例えば、図３６Ａ及び図３６Ｂに示すように、不揮発性メモリ３４の上に保護アルミニウム層３５１を形成し、さらに、その保護アルミニウム層３５１と同一平面上となるように、不揮発性メモリ３４にバッテリ３１３からの電力を供給する電源パターン３５２を形成するようにすることができる。このようにすると、例えば、不揮発性メモリ３４を改竄すべく、保護アルミニウム層３５１を削除しようとすると、同一平面上の電源パターン３５２も削除されてしまい、不揮発性メモリ３４に対する電力の供給が断たれ、内部に記憶されているデータが消去されてしまうことになる。このように構成することで、タンパーレジスト性をより高めることができる。

さらに、図３７に示すように、不揮発性メモリ３４に対するデータの書き込み又は読み出しのための配線４０１－１乃至４０１－３は、対応する位置で、上下（深さ）方向に重なりあうように形成されている。これにより、より下層の配線４０１－３からデータを読み出すためには、上方の配線４０１－１，４０１－２を除去しなければならず、複数の配線４０１－１，４０１－２，４０１－３から同時にデータを読み取ることができなくなる。

さらにまた、不揮発性メモリ３４は、配線４０１－１乃至４０１－３を冗長に形成するようにすることができる。例えば、不揮発性メモリ３４内部に形成される配線４０１－１乃至４０１－３が不揮発性メモリ３４を構成するトランジスタなどの素子を結合するとき、その経路は、例え、直線的に結合が可能であっても、直線的には形成されず、所定の長さとなるように形成される。このようにするこ

とで、配線４０１－１乃至４０１－３の長さは、本来必要な長さ以上の長さとなり、配線に必要な最短の長さの場合に比較して大きな寄生容量を有することとなる。

不揮発性メモリ３４からデータを読み出すために設計されている専用の回路（半導体ＩＣとしてのアダプタ２６に内蔵されている）は、その寄生容量にマッチングしたインピーダンスを設定することで、不揮発性メモリ３４が記憶しているデータを正常に読み出すことができる。しかしながら、不揮発性メモリ３４に記憶されているデータを読み出すべく、プローブを配線４０１－１乃至４０１－３に接続させると、その寄生容量とプローブによる合成の容量が影響して、データを正常に読み出すことが困難になる。

次に、ポータブルデバイス６がパーソナルコンピュータ１から所定のデータを受け取る場合の、相互認証の処理を図３８及び図３９のフローチャートを参照して説明する。ステップＳ４０１において、パーソナルコンピュータ１のＣＰＵ１１は、乱数Ｎａを生成する。ステップＳ４０２において、パーソナルコンピュータ１のＣＰＵ１１は、インターフェース１７に、パーソナルコンピュータ１のＩＤ、鍵のカテゴリ番号Ｇ及び乱数Ｎａをポータブルデバイス６へ送信させる。

ステップＳ４２１において、ポータブルデバイス６のＣＰＵ５３は、乱数Ｎｂを生成する。ステップＳ４２２において、ポータブルデバイス６は、パーソナルコンピュータ１からインターフェース１７を介して送信されたパーソナルコンピュータ１のＩＤ、鍵のカテゴリ番号Ｇ及び乱数Ｎａを受信する。ステップＳ４２３において、ポータブルデバイス６のＣＰＵ５３は、鍵のカテゴリ番号Ｇから、

マスター鍵ＫＭａの鍵番号ｊを求める。

ステップＳ４２４において、ポータブルデバイス６のＣＰＵ５３は、ｊ番目のマスター鍵ＫＭａ［ｊ］を求める。ステップＳ４２５において、ポータブルデバイス６のＣＰＵ５３は、パーソナルコンピュータ１のＩＤに、マスター鍵ＫＭａ［ｊ］を基にしたＳＨＡなどのハッシュ関数を適用し、鍵Ｋａｂを求める。

ステップＳ４２６において、ポータブルデバイス６のＣＰＵ５３は、乱数Ｎａ、乱数Ｎｂ及びパーソナルコンピュータ１のＩＤに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用し、乱数Ｒ１を求める。ステップＳ４２７において、ポータブルデバイス６のＣＰＵ５３は、乱数Ｓｂを生成する。

ステップＳ４２８において、ポータブルデバイス６のＣＰＵ５３は、ＵＳＢコントローラ５７に、乱数Ｎａ、乱数Ｎｂ、鍵番号ｊ及び乱数Ｓｂをパーソナルコンピュータ１へ送信させる。

ステップＳ４０３において、パーソナルコンピュータ１は、インターフェース１７を介して、乱数Ｎａ、乱数Ｎｂ、鍵番号ｊ及び乱数Ｓｂを受信する。ステップＳ４０４において、パーソナルコンピュータ１のＣＰＵ１１は、鍵番号ｊを基に、個別鍵ＫＩａに含まれる鍵Ｋａｂを求める。ステップＳ４０５において、パーソナルコンピュータ１のＣＰＵ１１は、乱数Ｎａ、乱数Ｎｂ及びパーソナルコンピュータ１のＩＤに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用し、乱数Ｒ２を求める。

ステップＳ４０６において、パーソナルコンピュータ１のＣＰＵ１１は、受信した乱数Ｒ１と、ステップＳ４０５で生成した乱数Ｒ２とが等しいか否かを判定し、乱数Ｒ１と乱数Ｒ２とが等しくない

と判定された場合、正当なポータブルデバイスではないので、ポータブルデバイス６を認証せず、処理は終了する。ステップＳ４０６において、乱数Ｒ１と乱数Ｒ２とが等しいと判定された場合、ポータブルデバイス６は正当なポータブルデバイスなので、ステップＳ４０７に進み、パーソナルコンピュータ１のＣＰＵ１１は、乱数Ｓａを生成する。

ステップＳ４０８において、パーソナルコンピュータ１のＣＰＵ１１は、乱数Ｎｂ及び乱数Ｎａに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用し、乱数Ｒ３を求める。ステップＳ４０９において、パーソナルコンピュータ１のＣＰＵ１１は、インターフェース１７に、乱数Ｒ３及び乱数Ｓｂをポータブルデバイス６へ送信させる。ステップＳ４１０において、パーソナルコンピュータ１のＣＰＵ１１は、乱数Ｓａ及び乱数Ｓｂに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用し、一時鍵Ｋｓを求める。

ステップＳ４２９において、ポータブルデバイス６のＣＰＵ５３は、乱数Ｒ３及び乱数Ｓｂを受信する。ステップＳ４３０において、ポータブルデバイス６のＣＰＵ５３は、乱数Ｎｂ及び乱数Ｎａに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用し、乱数Ｒ４を求める。ステップＳ４３１において、ポータブルデバイス６のＣＰＵ５３は、受信した乱数Ｒ３と、ステップＳ４３０で生成した乱数Ｒ４とが等しいか否かを判定し、乱数Ｒ３と乱数Ｒ４とが等しくないと判定された場合、正当なパーソナルコンピュータではないので、パーソナルコンピュータ１を認証せず、処理は終了する。ステップＳ４３１において、乱数Ｒ３と乱数Ｒ４とが等しいと判定された場合、パーソナルコンピュータ１は正当なパーソナルコンピュー

タなので、ステップＳ４３２に進み、ポータブルデバイス６のＣＰＵ５３は、乱数Ｓａ及び乱数Ｓｂに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用し、一時鍵Ｋｓを求める。

以上のように、パーソナルコンピュータ１及びポータブルデバイス６は、相互認証し、共通の一時鍵Ｋｓを得る。なお、ステップＳ４２５、ステップＳ４２６、ステップＳ４０５、ステップＳ４０８、ステップＳ４１０、ステップＳ４３０及びステップＳ４３２において、ＳＨＡなどのハッシュ関数を適用するとして説明したが、ＤＥＳなどを適用しても良い。

次に、パーソナルコンピュータ１がポータブルデバイス６に所定のデータを送信する場合の、相互認証の処理を図４０及び図４１のフローチャートを参照して説明する。ステップＳ４５１において、パーソナルコンピュータ１のＣＰＵ１１は、乱数Ｎａを生成する。ステップＳ４５２において、パーソナルコンピュータ１は、インターフェース１７を介して、パーソナルコンピュータ１のＩＤ、パーソナルコンピュータ１の鍵のカテゴリ番号Ｇｐ、ポータブルデバイス６の鍵のカテゴリ番号Ｇｓ及び乱数Ｎａをポータブルデバイス６に送信する。

ステップＳ４８１において、ポータブルデバイス６のＣＰＵ５３は、乱数Ｎｂを生成する。ステップＳ４８２において、ポータブルデバイス６は、パーソナルコンピュータ１からインターフェース１７を介して送信されたパーソナルコンピュータ１のＩＤ、パーソナルコンピュータ１の鍵のカテゴリ番号Ｇｐ、ポータブルデバイス６の鍵のカテゴリ番号Ｇｓ及び乱数Ｎａを受信する。ステップＳ４８３において、ポータブルデバイス６のＣＰＵ５３は、ポータブルデ

バイス６の鍵のカテゴリ番号Ｇｓから、マスター鍵ＫＭａの鍵番号ｊを求める。

ステップＳ４８４において、ポータブルデバイス６のＣＰＵ５３は、ｊ番目のマスター鍵ＫＭａ［ｊ］を求める。ステップＳ４８５において、ポータブルデバイス６のＣＰＵ５３は、パーソナルコンピュータ１のＩＤに、マスター鍵ＫＭａ［ｊ］を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、鍵Ｋａｂを求める。ステップＳ４８６において、ポータブルデバイス６のＣＰＵ５３は、パーソナルコンピュータ１の鍵のカテゴリ番号Ｇｐを基に、マスター鍵ＫＩａの鍵番号ｋを求める。ステップＳ４８７において、ポータブルデバイス６のＣＰＵ５３は、鍵Ｋａｂに、マスター鍵ＫＩａ［ｋ］を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、鍵Ｋ’ａｂを求める。

ステップＳ４８８において、ポータブルデバイス６のＣＰＵ５３は、乱数Ｎａ及び乱数Ｎｂに、鍵Ｋ’ａｂを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、乱数Ｒ１を求める。ステップＳ４８９において、ポータブルデバイス６のＣＰＵ５３は、乱数Ｓｂを生成する。

ステップＳ４９０において、ポータブルデバイス６のＣＰＵ５３は、ＵＳＢコントローラ５７に、ポータブルデバイス６のＩＤ、乱数Ｎｂ、乱数Ｒ１、鍵番号ｊ及び乱数Ｓｂをパーソナルコンピュータ１へ送信させる。

ステップＳ４５３において、パーソナルコンピュータ１は、インターフェース１７を介して、ポータブルデバイス６のＩＤ、乱数Ｎｂ、乱数Ｒ１、鍵番号ｊ及び乱数Ｓｂを受信する。ステップＳ４５

４において、パーソナルコンピュータ１のＣＰＵ１１は、ポータブルデバイス６のＩＤに、パーソナルコンピュータ１のマスター鍵ＫＭＰを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、マスター鍵Ｋｍを求める。ステップＳ４５５において、パーソナルコンピュータ１のＣＰＵ１１は、ｊ番目の個別鍵ＫＩａを求める。ステップＳ４５６において、パーソナルコンピュータ１のＣＰＵ１１は、乱数Ｎａ及び乱数Ｎｂに、鍵ＫＩａを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、鍵Ｋ’ａｂを求める。ステップＳ４５７において、パーソナルコンピュータ１のＣＰＵ１１は、乱数Ｎａ及び乱数Ｎｂに、鍵Ｋ’ａｂを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、乱数Ｒ２を求める。

ステップＳ４５８において、パーソナルコンピュータ１のＣＰＵ１１は、受信した乱数Ｒ１と、ステップＳ４５７で生成した乱数Ｒ２とが等しいか否かを判定し、乱数Ｒ１と乱数Ｒ２とが等しくないと判定された場合、正当なポータブルデバイスではないので、ポータブルデバイス６を認証せず、処理は終了する。ステップＳ４５８において、乱数Ｒ１と乱数Ｒ２とが等しいと判定された場合、ポータブルデバイス６は正当なポータブルデバイスなので、ステップＳ４５９に進み、パーソナルコンピュータ１のＣＰＵ１１は、乱数Ｓａを生成する。

ステップＳ４６０において、パーソナルコンピュータ１のＣＰＵ１１は、乱数Ｎｂ及び乱数Ｎａに、鍵ＫＩａを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、乱数Ｒ３を求める。ステップＳ４６１において、パーソナルコンピュータ１のＣＰＵ１

１は、インターフェース１７を介して、ポータブルデバイス６に、乱数Ｒ３及び乱数Ｓｂを送信する。ステップＳ４６２において、パーソナルコンピュータ１のＣＰＵ１１は、乱数Ｓａ及び乱数Ｓｂに、鍵Ｋ’ａｂを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、一時鍵Ｋｓを求める。

ステップＳ４９１において、ポータブルデバイス６のＣＰＵ５３は、乱数Ｒ３及び乱数Ｓｂを受信する。ステップＳ４９２において、ポータブルデバイス６のＣＰＵ５３は、乱数Ｎｂ及び乱数Ｎａに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、乱数Ｒ４を求める。ステップＳ４９３において、ポータブルデバイス６のＣＰＵ５３は、受信した乱数Ｒ３と、ステップＳ４９２で生成した乱数Ｒ４とが等しいか否かを判定し、乱数Ｒ３と乱数Ｒ４とが等しくないと判定された場合、正当なパーソナルコンピュータではないので、パーソナルコンピュータ１を認証せず、処理は終了する。ステップＳ４９３において、乱数Ｒ３と乱数Ｒ４とが等しいと判定された場合、パーソナルコンピュータ１は、正当なパーソナルコンピュータなので、ステップＳ４９４に進み、ポータブルデバイス６のＣＰＵ５３は、乱数Ｓａ及び乱数Ｓｂに、鍵Ｋａｂを基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、一時鍵Ｋｓを求める。

このように、パーソナルコンピュータ１及びポータブルデバイス６は、相互認証し、共通の一時鍵Ｋｓを得る。図４０及び図４１のフローチャートに示した手続は、図３８及び図３９のフローチャートに示す手続よりも、いわゆる”なりすまし”に対する防御（検出）が強力である。なお、ステップＳ４８５、ステップＳ４８７、

ステップＳ４８８、ステップＳ４５４、ステップＳ４５６、ステップＳ４５７、ステップＳ４６０、ステップＳ４６２、ステップＳ４９２及びステップＳ４９４において、ＳＨＡなどのハッシュ関数を適用するとして説明したが、ＤＥＳなどを適用しても良い。

以上のように、パーソナルコンピュータ１及びポータブルデバイス６は、相互認証の後に行われる処理に対応し、検出力が異なる相互認証の手続を使い分けることにより、効率的かつ強力に、なりすましによる攻撃に対応することができる。

次に、ソースプログラムを暗号化する処理を、図４２のフローチャートを参照して説明する。ステップＳ５０１において、パーソナルコンピュータ１は、通信部２５を介して、図示せぬ認証局に署名を付したソースプログラムを送信する。ステップＳ５０２において、認証局は、署名を基に、受信したソースプログラムに改竄が発見されたか否かを判定し、受信したソースプログラムに改竄が発見された場合、処理は継続できないので、処理は終了する。

ステップＳ５０２において、受信したソースプログラムに改竄が発見さなかった場合、ステップＳ５０３に進み、認証局は、受信したソースプログラムを認証局の秘密鍵で暗号化する。ステップＳ５０４において、認証局は、暗号化したソースプログラムをパーソナルコンピュータ１に送信する。ステップＳ５０５において、パーソナルコンピュータ１は、受信したソースプログラムを、ＨＤＤ２１に記録し、処理は終了する。

以上のように、ソースプログラムは、暗号化される。なお、認証局に代わり、ＥＭＤサーバ４－１乃至４－３又は所定の安全なサーバが、ソースプログラムを暗号化するようにしてもよい。

次に、暗号化されたソースプログラムをアダプタ２６が実行する処理を、図４３のフローチャートを参照して説明する。ステップＳ５２１において、アダプタ２６のＣＰＵ３２は、パーソナルコンピュータ１から受信した、暗号化されたソースプログラムを、不揮発性メモリ３４に予め記憶されている認証局の公開鍵で復号する。ステップＳ５２２において、アダプタ２６のＣＰＵ３２は、インタープリタを起動し、復号されたソースプログラムを実行する。

ステップＳ５２３において、アダプタ２６のＣＰＵ３２は、ソースプログラムを実行して得られた結果を、パーソナルコンピュータ１に送信するか否かを判定し、結果をパーソナルコンピュータ１に送信しないと判定された場合、処理は終了する。ステップＳ５２３において、結果をパーソナルコンピュータ１に送信すると判定された場合、ステップＳ５２４に進み、アダプタ２６のＣＰＵ３２は、ソースプログラムを実行して得られた結果を所定の鍵で暗号化する。ステップＳ５２５において、アダプタ２６のＣＰＵ３２は、インターフェース３１を介して、暗号化された結果をパーソナルコンピュータ１に送信し、処理は終了する。

以上のように、アダプタ２６は、暗号化されたソースプログラムを実行し、所定の場合、得られた結果を暗号化し、パーソナルコンピュータ１に送信する。

なお、オブジェクトプログラムを暗号化し、暗号化されたオブジェクトプログラムをアダプタ２６が実行するようにしてもよい。図４４は、オブジェクトプログラムを暗号化する処理を説明するフローチャートである。ステップＳ５４１において、パーソナルコンピュータ１は、ソースプログラムをコンパイルし、所定のオブジェク

トプログラムを生成する。ステップＳ５４２乃至ステップＳ５４６の処理は、図４２のステップＳ５０１乃至ステップＳ５０５とそれぞれ同様の処理なので、その説明は省略する。

図４５は、暗号化されたオブジェクトプログラムをアダプタ２６が実行する処理を説明するフローチャートである。ステップＳ５６１において、アダプタ２６のＣＰＵ３２は、パーソナルコンピュータ１から受信した、暗号化されたオブジェクトプログラムを、不揮発性メモリ３４に予め記憶されている認証局の公開鍵で復号する。ステップＳ５６２において、アダプタ２６のＣＰＵ３２は、復号されたオブジェクトプログラムをＲＡＭ３３に展開し、実行する。ステップＳ５６３乃至ステップＳ５６５は、図４３のステップ５２３乃至ステップＳ５２５とそれぞれ同様の処理なので、その説明は省略する。

次に、オブジェクトプログラムを暗号化する他の処理を、図４６のフローチャートを参照して説明する。ステップＳ５８１において、パーソナルコンピュータ１のＣＰＵ１１は、ソースプログラムをコンパイルし、オブジェクトプログラムを生成する。ステップＳ５８２において、パーソナルコンピュータ１のＣＰＵ１１は、インターフェース１７を介して、アダプタ２６にアプリケーション鍵Ｋａｐ及び個別鍵Ｋｉｄｖの発行を要求する。

ステップＳ５８３において、パーソナルコンピュータ１は、インターフェース１７を介して、アダプタ２６からアプリケーション鍵Ｋａｐ及び個別鍵Ｋｉｄｖ（アダプタ２６の不揮発性メモリ３４に記憶されている、アダプタ２６固有の鍵Ｋｓを基に、生成される）を受信する。ステップＳ５８４において、パーソナルコンピュータ

１のＣＰＵ１１は、オブジェクトプログラムをアプリケーション鍵Ｋａｐで暗号化する。ステップＳ５８５において、パーソナルコンピュータ１のＣＰＵ１１は、コンテキストに含まれるマスター鍵ＫＭｂなどを個別鍵Ｋｉｄｖで暗号化する。ステップＳ５８６において、パーソナルコンピュータ１のＣＰＵ１１は、アプリケーション鍵Ｋａｐで暗号化されたオブジェクトプログラム及び個別鍵Ｋｉｄｖで暗号化されたコンテキストに含まれるマスター鍵ＫＭｂなどをＨＤＤ２１に記録させ、処理は終了する。

このように、パーソナルコンピュータ１は、アダプタ２６から供給されたアプリケーション鍵Ｋａｐ及び個別鍵Ｋｉｄｖで、オブジェクトプログラム及びコンテキストを暗号化することができる。

図４６のフローチャートに示される手順で暗号化されたオブジェクトプログラムをアダプタ２６が実行する処理を、図４７のフローチャートを参照して説明する。ステップＳ６０１において、パーソナルコンピュータ１のＣＰＵ１１は、インターフェース１７を介して、アダプタ２６に、アプリケーション鍵Ｋａｐで暗号化されたオブジェクトプログラム及び個別鍵Ｋｉｄｖで暗号化されたコンテキストに含まれるマスター鍵ＫＭｂなどを送信する。

ステップＳ６０２において、アダプタ２６のＣＰＵ３２は、不揮発性メモリ３４に予め記憶されている鍵Ｋｓ及びアプリケーション鍵Ｋａｐに、ハッシュ関数を適用し、個別鍵Ｋｉｄｖを生成する。ステップＳ６０３において、アダプタ２６のＣＰＵ３２は、受信したオブジェクトプログラムをアプリケーション鍵Ｋａｐで復号する。ステップＳ６０４において、アダプタ２６のＣＰＵ３２は、コンテキストに含まれるマスター鍵ＫＭｂなどを個別鍵Ｋｉｄｖで復号す

る。

ステップＳ６０５において、アダプタ２６のＣＰＵ３２は、復号されたマスター鍵ＫＭｂなどを含むコンテキストを利用して、オブジェクトプログラムを実行する。ステップＳ６０６乃至ステップＳ６０８の処理は、図４３のステップＳ５２３乃至ステップＳ５２５とそれぞれ同様なので、その説明は省略する。

以上のように、図４７のフローチャートで示される処理において、図４６のフローチャートで個別鍵Ｋｉｄｖを送信したアダプタ２６は、暗号化されたオブジェクトプログラムを実行することができる。従って、図４６のフローチャートで個別鍵Ｋｉｄｖを送信したアダプタ２６以外のアダプタは、オブジェクトプログラムを復号できるが、コンテキストを復号できず、暗号化されたオブジェクトプログラムは実行できない。

次に、アダプタ２６がオブジェクトプログラムを実行する場合、処理の一部をパーソナルコンピュータ１のＣＰＵ１１に実行させるときの処理を図４８のフローチャートを参照して説明する。ステップＳ６５１において、アダプタ２６のＣＰＵ３２は、オブジェクトプログラムの所定の命令列を、所定の規則に従って、変換する。

この変換は、例えば、ＤＥＳの暗号化又は復号のプログラムの場合、Feistel 構造などの基本構造を繰り返す処理のとき、いわゆるＦ関数で利用される４８ビットの拡大鍵と適切な乱数とに排他的論理和を所定の回数、適用するなどの変換を実行し、拡大鍵を解読しにくくする。また、例えば、ＤＥＳ　ＣＢＣ(Cipher Block Chaining) Ｍｏｄｅで、多量のデータを復号するプログラムの場合、繰り返し構造の処理を順（シーケンシャル）に実行せず、多量のデータ

に対し、複数の繰り返し構造の処理を同時に実行し、拡大鍵を解読しにくくする。

また、例えば、ソースプログラムのインストラクションに対応するコード（例えば、加算を表すコードが”１”に対応し、乗算を表すコードが”２”に対応する）を毎回変更する。

ステップＳ６５２において、アダプタ２６のＣＰＵ３２は、変換された命令列を、インターフェース３１を介して、パーソナルコンピュータ１に送信する。

ステップＳ６５３において、パーソナルコンピュータ１のＣＰＵ１１は、デシャッフルされた命令列を実行する。ステップＳ６５４において、パーソナルコンピュータ１のＣＰＵ１１は、命令列を実行して得られた処理結果をアダプタ２６に送信する。

ステップＳ６５５において、アダプタ２６のＣＰＵ３２は、パーソナルコンピュータ１から受信した処理結果及びアダプタ２６のＣＰＵ３２が算出し保持している計算結果を基に、処理を継続する。ステップＳ６５６において、アダプタ２６のＣＰＵ３２は、パーソナルコンピュータ１に処理を実行させるか否かを判定し、パーソナルコンピュータ１に処理を実行させないと判定された場合、処理は終了する。ステップＳ６５６において、パーソナルコンピュータ１に処理を実行させると判定された場合、手続は、ステップＳ６５１に戻り、パーソナルコンピュータ１に処理を実行させる処理を繰り返す。

以上のように、アダプタ２６は、オブジェクトプログラムの処理の一部をパーソナルコンピュータ１に実行させることにより、高速にかつ安全に、オブジェクトプログラムの処理を実行することがで

きる。

アダプタ２６は、オブジェクトプログラムに含まれる命令列を変換してパーソナルコンピュータ１に送信することにより、オブジェクトプログラムの解読が困難になる。アダプタ２６が、オブジェクトプログラムに含まれる命令列を暗号化して、パーソナルコンピュータ１に送信すれば、オブジェクトプログラムの解読は更に困難になる。

なお、図４６で説明したパーソナルコンピュータ１がアダプタ２６に供給するオブジェクトプログラムを暗号化する処理において、ソースプログラムに対しステップＳ６５１に示した変換を実行すれば、オブジェクトプログラムの解読は更に困難になる。

最後に、パーソナルコンピュータ１がＥＭＤサーバ４－１乃至４－３から、事前に無料でダウンロードした音楽データを暗号化している暗号鍵をダウンロードするとともに、決済をする処理を、図４９のフローチャートを参照して説明する。ステップＳ６７１において、パーソナルコンピュータ１は、ネットワーク２を介してＥＭＤサーバ４－１乃至４－３と相互認証する。ステップＳ６７２において、パーソナルコンピュータ１のＣＰＵ１１は、通信部２５を介して、ＥＭＤサーバ４－１乃至４－３に、音楽データの再生条件を示すデータを送信する。ステップＳ６７３において、ＥＭＤサーバ４－１乃至４－３は、受信した再生条件を示すデータを基に、支払金額のデータをパーソナルコンピュータ１に送信する。

ステップＳ６７４において、パーソナルコンピュータ１のＣＰＵ１１は、ＥＭＤサーバ４－１乃至４－３から受信した支払金額のデータをディスプレイ２０に表示させる。ステップＳ６７５において、

ＥＭＤサーバ４－１乃至４－３は、パーソナルコンピュータ１に、ユーザのクレジットカードの番号等の送信を要求する。ステップＳ６７６において、ユーザは、キーボード１８又はマウス１９を操作し、パーソナルコンピュータ１にクレジットカードの番号等のデータを入力し、パーソナルコンピュータ１は、クレジットカードの番号等のデータをＥＭＤサーバ４－１乃至４－３に送信する。

ステップＳ６７７において、ＥＭＤサーバ４－１乃至４－３は、パーソナルコンピュータ１から受信したクレジットカードの番号等のデータを基に、決済の処理を実行する。ステップＳ６７８において、ＥＭＤサーバ４－１乃至４－３は、ネットワーク２を介して、パーソナルコンピュータ１に所定の暗号鍵を送信する。ステップＳ６７９において、パーソナルコンピュータ１は、ネットワーク２を介して、ＥＭＤサーバ４－１乃至４－３から送信された所定の暗号鍵を受信し、処理は終了する。

以上のように、パーソナルコンピュータ１がＥＭＤサーバ４－１乃至４－３から暗号鍵をダウンロードするとともに、ＥＭＤサーバ４－１乃至４－３は、決済の処理をすれば、パーソナルコンピュータ１がＥＭＤサーバ４－１乃至４－３から音楽データをダウンロードするとき、認証、暗号化、又は決済などの処理が必要なくなるので、比較的大きなデータである音楽データを迅速にダウンロードすることができる。

以上においては、記録媒体として、ポータブルデバイス６を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転又はコピーする場合にも応用することが可能である。クレジットカードの番号等のデータを基に、決済の処理を実行するとし

て説明したが、ｓｍａｓｈ（商標）などの手続により、決済をするようにしてもよい。

また、図４９のフローチャートに示す処理の前に、パーソナルコンピュータ１とＥＭＤサーバ４－１乃至４－３とが、例えば、ＩＳＯ９７９８－３で規定されているｈｔｔｐ(Hypertext Transport Protocol)上のプロトコルを使用して、相互認証するようにしてもよい。

なお、ポータブルデバイス６は、予め個別鍵を記憶しているして説明したが、ユーザがポータブルデバイス６を購入後、ＥＭＤサーバ４－１乃至４－３などからダウンロードするようにしてもよい。

また、データは、音楽データ以外に、画像データ、その他のデータとすることもできる。

以上においては、記録媒体として、ポータブルデバイス６を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転又はコピーする場合にも応用することが可能である。また、コンテンツは、曲のデータ又は音声データなどの楽音データ以外に、画像データ、その他のデータとすることもできる。

このように、本発明によれば、次のような効果を奏することができる。

（１）　ＨＤＤ２１に暗号化してデータを記録するとともに、暗号鍵も保存用鍵で暗号化した上でＨＤＤ２１に記録するようにしたので、ＨＤＤ２１に記録されているコンテンツをコピーしても、これを復号することができないので、複製が大量に配布されることを防止することができる。

（２）　所定の曲を１回コピーしたとき、一定時間（上記例の場

合、４８時間）の間、その曲をコピーすることができないようするために、その曲と録音日時を曲データベース上に登録するようにしたので、そのコピー回数を制限することができ、複製を大量に配布することを防止することができる。

さらにデータベースを更新するたびに、データのハッシュ値を計算し保存するようにしたので、データベースの改竄を防止することが容易となる。

（３）　外部の装置にコンテンツを渡したら、ＨＤＤ２１上のコンテンツを消去するようにしたので、ＨＤＤ２１内に元のデジタルデータであるコンテンツが残らず、その複製を大量に配布することが防止される。

（４）　ＨＤＤ２１内に曲データベースを設け、全体のハッシュ値を毎回チェックするようにしたので、ＨＤＤ２１の内容をムーブの直前にバックアップし、ムーブ直後にバックアップしたデータをＨＤＤ２１にリストアするようにしたとしても、送り元のデータを確実に消去することが可能となる。

（５）　パーソナルコンピュータ１が外部の機器にデータを渡すとき、その前に相互認証処理を行うようにしたので、不正な機器にデータを渡してしまうようなことが防止される。

（６）　外部機器から、パーソナルコンピュータ１に対してデータを渡す前に、パーソナルコンピュータ１のソフトウェアが正当なものであるか否かを相互認証により確認するようにしたので、不正なソフトウェアに対してコンテンツを渡してしまうようなことが防止される。

（７）　曲の同一性の判定にＩＳＲＣを用い、ＩＳＲＣが取得で

きないときは、ＴＯＣを用いるようにしたので、ＩＳＲＣが取得できなくとも、曲の同一性を判定することが可能になる。

（８）　パーソナルコンピュータ１におけるソフトウェア機能のうち、所定の部分をパーソナルコンピュータ１に外付けされるアダプタ２６に負担させるようにしたので、パーソナルコンピュータ１のソフトウェアを解析しただけでは、全体としてどのような処理となっているのかが判らないので、ソフトウェアを改竄をして、意図する機能を持たせるようなことが困難となる。

更に、そのソフトウェアが、安全な認証局又はＥＭＤサーバ４－１乃至４－３で暗号化又はシャッフルされるので、ソフトウェアの改竄は、より困難となる。

（９）　プログラムをプログラムに対応する鍵で暗号化し、プログラムの実行に必要なデータを、アダプタ２６が生成する固有の鍵で暗号化するようにしたので、プログラムのみをＣＤ－ＲＯＭなどの媒体で配布可能にしつつ、プログラムを他のアダプタ２６で実行することが防止される。

（１０）　音楽データなどのコンテンツを暗号化する鍵をダウンロードするとき、決済されるようにしたので、比較的大きなデータである音楽データなどのコンテンツを迅速にダウンロードすることができるようになる。

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

なお、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、ＣＤ－ＲＯＭ、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体

を利用することができる。

以上のように、本発明に係る情報提供装置、情報提供方法及びプログラム提供媒体では、情報処理装置から所定のプログラムが受信されるとともに、暗号化されたプログラムが情報処理装置に送信され、受信したプログラムが暗号化されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体では、所定の処理に対応し、１以上の相互認証の手続から、実行する相互認証の処理が選択され、選択された相互認証の手続が実行されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報提供装置、情報提供方法及びプログラム提供媒体では、情報処理装置から、情報処理装置がダウンロードしたデータの利用に関するデータ及び決済に必要なデータが受信されるとともに、情報処理装置に、鍵が送信され、情報処理装置から受信したデータの利用に関するデータ及び決済に必要なデータを基に、決済されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体によれば、暗号化されているプログラムが復号され実行され、プログラムが供給されるとともに、暗号化されているプログラムが復号され、実行の結果を基に、プログラムが実行されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体では、半導体ＩＣに実行させるプログラムが認証局に送信されるとともに、認証局から暗号化されたプログラムが受信され、認証局から受信した、暗号化されたプログラムが記録され、記録されているプログラムが、半導体ＩＣに送信されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理システムでは、半導体ＩＣに実行させるプログラムが認証局に送信されるとともに、認証局から暗号化されたプログラムが受信され、認証局から受信した、暗号化されたプログラムが記録され、記録されているプログラムが、半導体ＩＣに送信され、半導体ＩＣに実行させるプログラムが受信されるとともに、情報処理装置に暗号化されたプログラムが送信され、受信したプログラムが所定の方式で暗号化されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体では、半導体ＩＣに実行させるプログラムに含まれる命令列が並び替えられ、命令列が並び替えられたプログラムが記録され、記録されているプログラムが、半導体ＩＣに送信されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体では、半導体ＩＣに実行させるプログラムに含まれる命令列が並び替えられ、プログラムが暗号化され、命令列が並び替えら

れ、暗号化されたプログラムが記録され、記録されているプログラムが、半導体ＩＣに送信されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体では、プログラム及びプログラムの実行に必要なデータが蓄積され、プログラム及びデータの蓄積又は読み出しが制御され、プログラムが半導体ＩＣから供給された第１の鍵で暗号化され、データが半導体ＩＣから供給された第２の鍵で暗号化されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る半導体ＩＣ、情報処理方法及びプログラム提供媒体によれば、情報処理装置から転送されてくる暗号化されている第１のプログラムが受信され、受信された第１のプログラムが復号され、復号された第１のプログラムを処理する第２のプログラムが保持され、保持されている第２のプログラムに基づいて処理された第１のプログラムが実行され、実行した結果が情報処理装置に転送され、計時動作を行うとともに、情報処理装置からの時刻情報に基づいて、現在時刻が修正されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る情報処理装置、情報処理方法及びプログラム提供媒体では、半導体ＩＣに暗号化されているプログラムが送信され、半導体ＩＣが、プログラムを処理した結果生成し、出力したデータが受信され、他の装置からデータと時刻情報が受信され、受信したデータが蓄積され、受信した時刻情報に基づいて、半導体ＩＣ

の時刻情報が修正されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

また、本発明に係る半導体ＩＣ、情報処理方法、プログラム提供媒体では、半導体ＩＣ固有の第１の鍵が予め記憶され、記憶している第１の鍵及び情報処理装置から供給されたプログラムの属性から、第２の鍵が生成され、プログラムが第３の鍵で復号され、データが第２の鍵で復号されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

さらに、本発明に係る情報処理システムによれば、プログラム及びプログラムの実行に必要なデータが蓄積され、プログラム及びデータの蓄積又は読み出しが制御され、プログラムが半導体ＩＣから供給された第１の鍵で暗号化され、データが半導体ＩＣから供給された第２の鍵で暗号化され、暗号化されたプログラム及びプログラムの実行に必要なデータが半導体ＩＣに送信されるとともに、第１の鍵及び第２の鍵が半導体ＩＣから受信され、暗号化されたプログラム及びプログラムの実行に必要なデータが受信されるとともに、第１の鍵及び第２の鍵が情報処理装置に送信され、半導体ＩＣ固有の第３の鍵が予め記憶され、記憶している第３の鍵及び情報処理装置から供給されたプログラムの属性から、第２の鍵が生成され、受信したプログラムが第１の鍵で復号され、受信したデータが第２の鍵で復号されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

請求の範囲

1．　ネットワークを介して、所定の情報処理装置に接続されている情報提供装置において、

前記情報処理装置から所定のプログラムを受信するとともに、暗号化された前記プログラムを前記情報処理装置に送信する通信手段と、

通信手段が受信した前記プログラムを暗号化する暗号化手段と

を含むことを特徴とする情報提供装置。

2．　前記プログラムは、インタープリタに実行させるソースプログラムであることを特徴とする請求の範囲第1項に記載の情報提供装置。

3．　前記プログラムは、オブジェクトプログラムであることを特徴とする請求の範囲第1項に記載の情報提供装置。

4．　ネットワークを介して、所定の情報処理装置に接続されている情報提供装置の情報提供方法において、

前記情報処理装置から所定のプログラムを受信するとともに、暗号化された前記プログラムを前記情報処理装置に送信する通信ステップと、

通信ステップで受信した前記プログラムを暗号化する暗号化ステップと

を含むことを特徴とする情報提供方法。

5．　ネットワークを介して、所定の情報処理装置に接続されている情報提供装置に、

前記情報処理装置から所定のプログラムを受信するとともに、暗号化された前記プログラムを前記情報処理装置に送信する通信ステップと、

通信ステップで受信した前記プログラムを暗号化する暗号化ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

6． 他の情報処理装置と相互認証して、所定の処理を実行する情報処理装置において、

前記所定の処理に対応し、1以上の相互認証の手続から、実行する相互認証の処理を選択する選択手段と、

前記選択手段が選択された相互認証の手続を実行する相互認証手段と

を含むことを特徴とする情報処理装置。

7． 他の情報処理装置と相互認証して、所定の処理を実行する情報処理装置の情報処理方法において、

前記所定の処理に対応し、1以上の相互認証の手続から、実行する相互認証の処理を選択する選択ステップと、

前記選択ステップで選択された相互認証の手続を実行する相互認証ステップと

を含むことを特徴とする情報処理方法。

8． 他の情報処理装置と相互認証して、所定の処理を実行する情報処理装置に、

前記所定の処理に対応し、1以上の相互認証の手続から、実行する相互認証の処理を選択する選択ステップと、

前記選択ステップで選択された相互認証の手続を実行する相互認証ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

９．　第１装置において第１乱数を発生し、

第１装置の識別情報と鍵の属性情報と上記第１乱数とを第１装置から第２装置に送信し、

第２装置において第２乱数を発生し、

第２装置において上記第１装置から送信された第１装置の識別情報と鍵の属性情報と第１乱数とを受信し、

第２装置において上記鍵の属性情報から鍵を計算し、

第２装置において上記鍵と上記第１・第２乱数から第３乱数を発生し、

第２・第３乱数と鍵に関する情報とを第２装置から第１装置に送信し、

第１装置において上記第２装置から送信された第２・第３乱数と鍵に関する情報とを受信し、

第１装置において上記鍵に関する情報から鍵を生成し、

第１装置において上記鍵と上記第１・第２乱数から第４乱数を発生し、

上記第４乱数を第１装置から第２装置に送信し、

第１・第２装置の各々において第３・第４乱数と鍵とから一時鍵を求めることを特徴とする認証方法。

１０．　第１装置において第１乱数を発生し、

第１装置の識別情報と第１装置の鍵の属性情報と第２装置の鍵の

属性情報と上記第１乱数とを第１装置から第２装置に送信し、

第２装置において第２乱数を発生し、

第２装置において上記第１装置から送信された第１装置の識別情報と鍵の属性情報と第２装置の鍵の属性情報と上記第１乱数とを受信し、

第２装置において上記第２装置の鍵の属性情報から第１鍵を計算し、

第２装置において上記第１装置の鍵の属性情報から第２鍵を計算し、

第２装置において上記第２鍵と上記第１・第２乱数から第３乱数を発生し、

第２・第３乱数と鍵に関する情報とを第２装置から第１装置に送信し、

第１装置において上記第２装置から送信された第２・第３乱数と鍵に関する情報とを受信し、

第１装置において上記鍵に関する情報から第２鍵を生成し、

第１装置において上記第２鍵と上記第１・第２乱数から第４乱数を発生し、

上記第４乱数を第１装置から第２装置に送信し、

第１・第２装置の各々において第３・第４乱数と第２鍵とから一時鍵を求めることを特徴とする認証方法。

１１．　暗号化されている所定のデータ及び前記所定のデータを暗号化している鍵を情報処理装置に提供する情報提供装置において、

前記情報処理装置から、前記情報処理装置がダウンロードした前記データの利用に関するデータ及び決済に必要なデータを受信する

とともに、前記情報処理装置に、前記鍵を送信する通信手段と、

前記情報処理装置から受信した前記データの利用に関するデータ及び決済に必要なデータを基に、決済をする決済手段と

を含むことを特徴とする情報提供装置。

１２．　ｈｔｔｐ上のプロトコルを利用して、前記情報処理装置と相互認証する相互認証手段を更に含むことを特徴とする請求の範囲第１１項に記載の情報提供装置。

１３．　暗号化されている所定のデータ及び前記所定のデータを暗号化している鍵を情報処理装置に提供する情報提供装置の情報提供方法において、

前記情報処理装置から、前記情報処理装置がダウンロードした前記データの利用に関するデータ及び決済に必要なデータを受信するとともに、前記情報処理装置に、前記鍵を送信する通信ステップと、

前記情報処理装置から受信した前記データの利用に関するデータ及び決済に必要なデータを基に、決済をする決済ステップと

を含むことを特徴とする情報提供方法。

１４．　暗号化されている所定のデータ及び前記所定のデータを暗号化している鍵を情報処理装置に提供する情報提供装置に、

前記情報処理装置から、前記情報処理装置がダウンロードした前記データの利用に関するデータ及び決済に必要なデータを受信するとともに、前記情報処理装置に、前記鍵を送信する通信ステップと、

前記情報処理装置から受信した前記データの利用に関するデータ及び決済に必要なデータを基に、決済をする決済ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

１５．　暗号化されているプログラムを復号して実行する第１の実行手段と、

前記プログラムを前記第１の実行手段に供給するとともに、暗号化されている前記プログラムを復号し、前記第１の実行手段の実行の結果を基に、前記プログラムを実行する第２の実行手段と

を含むことを特徴とする情報処理装置。

１６．　前記第１の実行手段及び前記第２の実行手段は、それぞれ独立したハードウェアに設けられていることを特徴とする請求項１５に記載の情報処理装置。

１７．　前記プログラムは、インタープリタに実行させるソースプログラムであることを特徴とする請求の範囲第１５項に記載の情報処理装置。

１８．　前記プログラムは、オブジェクトプログラムであることを特徴とする請求の範囲第１５項に記載の情報処理装置。

１９．　暗号化されているプログラムを復号して実行する第１の実行ステップと、

前記プログラムを前記第１の実行ステップに供給するとともに、暗号化されている前記プログラムを復号し、前記第１の実行ステップの実行の結果を基に、前記プログラムを実行する第２の実行ステップと

を含むことを特徴とする情報処理装置の情報処理方法。

２０．　暗号化されているプログラムを復号して実行する第１の実行ステップと、

前記プログラムを前記第１の実行ステップに供給するとともに、暗号化されている前記プログラムを復号し、前記第１の実行ステッ

プの実行の結果を基に、前記プログラムを実行する第２の実行ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

２１．　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置において、

前記半導体ＩＣに実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信手段と、

前記認証局から受信した、暗号化された前記プログラムを記録する記録手段と、

前記記録手段に記録されている前記プログラムを、前記半導体ＩＣに送信する送信手段と

を含むことを特徴とする情報処理装置。

２２．　前記プログラムは、インタープリタに実行させるソースプログラムであることを特徴とする請求の範囲第２１項に記載の情報処理装置。

２３．　前記プログラムは、オブジェクトプログラムであることを特徴とする請求の範囲第２１項に記載の情報処理装置。

２４．　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置の情報処理方法において、

前記半導体ＩＣに実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信ステップと、

前記認証局から受信した、暗号化された前記プログラムを記録す

る記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップと

を含むことを特徴とする情報処理方法。

２５．　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置に、

前記半導体ＩＣに実行させる前記プログラムを認証局に送信するとともに、前記認証局から暗号化された前記プログラムを受信する通信ステップと、

前記認証局から受信した、暗号化された前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

２６．　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置及び認証局からなる情報処理システムにおいて、

前記情報処理装置は、前記半導体ＩＣに実行させる前記プログラムを認証局に送信するとともに、記認証局から暗号化された前記プログラムを受信する通信手段と、前記認証局から受信した、暗号化された前記プログラムを記録する記録手段と、前記記録手段に記録されている前記プログラムを、前記半導体ＩＣに送信する送信手段とを含み、

前記認証局は、前記半導体ＩＣに実行させる前記プログラムを受

信するとともに、前記情報処理装置に暗号化された前記プログラムを送信する通信手段と、前記通信手段が受信した前記プログラムを所定の方式で暗号化する暗号化手段とを含む

ことを特徴とする情報処理システム。

２７．　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置において、

前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替え手段と、

前記命令列が並び替えられた前記プログラムを記録する記録手段と、

前記記録手段に記録されている前記プログラムを、前記半導体ＩＣに送信する送信手段と

を含むことを特徴とする情報処理装置。

２８．　前記プログラムは、インタープリタに実行させるソースプログラムであることを特徴とする請求の範囲第２７項に記載の情報処理装置。

２９．　前記プログラムは、オブジェクトプログラムであることを特徴とする請求の範囲第２７項に記載の情報処理装置。

３０．　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置の情報処理方法において、

前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、

前記命令列が並び替えられた前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導

体ＩＣに送信する送信ステップと

を含むことを特徴とする情報処理方法。

３１．　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置に、

前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、

前記命令列が並び替えられた前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

３２．　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置において、

前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替え手段と、

前記プログラムを暗号化する暗号化手段と、

前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録手段と、

前記記録手段に記録されている前記プログラムを、前記半導体ＩＣに送信する送信手段と

を含むことを特徴とする情報処理装置。

３３．　前記プログラムは、インタープリタに実行させるソースプログラムであることを特徴とする請求の範囲第３２項に記載の情報処理装置。

３４．　前記プログラムは、オブジェクトプログラムであることを特徴とする請求の範囲第３２項に記載の情報処理装置。

３５．　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置の情報処理方法において、

前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、

前記プログラムを暗号化する暗号化ステップと、

前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップと

を含むことを特徴とする情報処理方法。

３６．　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置に、

前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、

前記プログラムを暗号化する暗号化ステップと、

前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

３７．　情報処理装置に装着され、前記情報処理装置からの指令に基づいて、各種の処理を実行する半導体ＩＣにおいて、

前記情報処理装置から転送されてくる暗号化されている第１のプログラムを受信する受信手段と、

前記受信手段により受信された前記第１のプログラムを復号する復号手段と、

前記復号手段により復号された前記第１のプログラムを処理する第２のプログラムを保持する保持手段と、

前記保持手段に保持されている前記第２のプログラムに基づいて処理された前記第１のプログラムを実行する実行手段と、

前記実行手段が実行した結果を前記情報処理装置に転送する転送手段と、

計時動作を行うとともに、前記情報処理装置からの時刻情報に基づいて、現在時刻を修正する計時手段と

を含むことを特徴とする半導体ＩＣ。

３８．　前記情報処理装置が利用するデータを記憶する不揮発性の記憶手段をさらに含むことを特徴とする請求の範囲第３７項に記載の半導体ＩＣ。

３９．　情報処理装置に装着され、前記情報処理装置からの指令に基づいて、各種の処理を実行する半導体ICの情報処理方法において、

前記情報処理装置から転送されてくる暗号化されている第１のプログラムを受信する受信ステップと、

前記受信ステップで受信された前記第１のプログラムを復号する復号ステップと、

前記復号ステップで復号された前記第１のプログラムを処理する第２のプログラムを保持する保持ステップと、

前記保持ステップの処理で保持された前記第２のプログラムに基

づいて処理された前記第１のプログラムを実行する実行ステップと、

前記実行ステップの処理で実行した結果を前記情報処理装置に転送する転送ステップと、

計時動作を行うとともに、前記情報処理装置からの時刻情報に基づいて、現在時刻を修正する計時ステップと

を含むことを特徴とする情報処理方法。

４０．　情報処理装置に装着され、前記情報処理装置からの指令に基づいて、各種の処理を実行する半導体ＩＣに、

前記情報処理装置から転送されてくる暗号化されている第１のプログラムを受信する受信ステップと、

前記受信ステップで受信された前記第１のプログラムを復号する復号ステップと、

前記復号ステップで復号された前記第１のプログラムを処理する第２のプログラムを保持する保持ステップと、

前記保持ステップの処理で保持された前記第２のプログラムに基づいて処理された前記第１のプログラムを実行する実行ステップと、

前記実行ステップの処理で実行した結果を前記情報処理装置に転送する転送ステップと、

計時動作を行うとともに、前記情報処理装置からの時刻情報に基づいて、現在時刻を修正する計時ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

４１．　装着された半導体ＩＣに各種の指令を出力し、実行させる情報処理装置において、

前記半導体ＩＣに暗号化されているプログラムを送信する送信手

段と、

前記半導体ＩＣが、前記プログラムを処理した結果生成し、出力したデータを受信する第１の受信手段と、

他の装置からデータと時刻情報を受信する第２の受信手段と、

前記第２の受信手段が受信したデータを蓄積する蓄積手段と、

前記第２の受信手段が受信した時刻情報に基づいて、前記半導体ＩＣの時刻情報を修正させる修正手段と

を含むことを特徴とする情報処理装置。

４２．　装着された半導体ＩＣに各種の指令を出力し、実行させる情報処理装置の情報処理方法において、

前記半導体ＩＣに暗号化されているプログラムを送信する送信ステップと、

前記半導体ＩＣが、前記プログラムを処理した結果生成し、出力したデータを受信する第１の受信ステップと、

他の装置からデータと時刻情報を受信する第２の受信ステップと、

前記第２の受信ステップで受信したデータを蓄積する蓄積ステップと、

前記第２の受信ステップで受信した時刻情報に基づいて、前記半導体ICの時刻情報を修正させる修正ステップと

を含むことを特徴とする情報処理方法。

４３．　装着された半導体ＩＣに各種の指令を出力し、実行させる情報処理装置に、

前記半導体ＩＣに暗号化されているプログラムを送信する送信ステップと、

前記半導体ＩＣが、前記プログラムを処理した結果生成し、出力

したデータを受信する第１の受信ステップと、

他の装置からデータと時刻情報を受信する第２の受信ステップと、

前記第２の受信ステップで受信したデータを蓄積する蓄積ステップと、

前記第２の受信ステップで受信した時刻情報に基づいて、前記半導体ＩＣの時刻情報を修正させる修正ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

４４．　所定の半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置において、

前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積手段と、

前記蓄積手段に対する前記プログラム及び前記データの蓄積又は読み出しを制御する制御手段と、

前記プログラムを前記半導体ＩＣから供給された第１の鍵で暗号化する第１の暗号化手段と、

前記データを前記半導体ＩＣから供給された第２の鍵で暗号化する第２の暗号化手段と

を含むことを特徴とする情報処理装置。

４５．　前記第１の鍵は、前記プログラムの属性で決定されることを特徴とする請求の範囲第４４項に記載の情報処理装置。

４６．　前記第２の鍵は、前記プログラムの属性及び前記半導体ＩＣが予め記憶している第３の鍵で決定される

ことを特徴とする請求の範囲第４４項に記載の情報処理装置。

４７．　所定の半導体ＩＣが装着され、前記半導体ＩＣに実行させ

るプログラムを供給する情報処理装置の情報処理方法において、

前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積ステップと、

前記蓄積ステップで前記プログラム及び前記データの蓄積又は読み出しを制御する制御ステップと、

前記プログラムを前記半導体ＩＣから供給された第１の鍵で暗号化する第１の暗号化ステップと、

前記データを前記半導体ＩＣから供給された第２の鍵で暗号化する第２の暗号化ステップと

を含むことを特徴とする情報処理方法。

４８．　所定の半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置に、

前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積ステップと、

前記蓄積ステップで前記プログラム及び前記データの蓄積又は読み出しを制御する制御ステップと、

前記プログラムを前記半導体ＩＣから供給された第１の鍵で暗号化する第１の暗号化ステップと、

前記データを前記半導体ＩＣから供給された第２の鍵で暗号化する第２の暗号化ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

４９．　所定の情報処理装置に装着し、前記情報処理装置から供給されたプログラム及び前記プログラムの実行に必要なデータを受信し、前記プログラムを実行する半導体ＩＣにおいて、

前記半導体ＩＣ固有の第１の鍵を予め記憶している記憶手段と、

前記記憶手段が記憶している前記第１の鍵及び前記情報処理装置から供給されたプログラムの属性から、第２の鍵を生成する鍵生成手段と、

前記プログラムを第３の鍵で復号する第１の復号手段と、

前記データを第２の鍵で復号する第２の復号手段と

を含むことを特徴とする半導体ＩＣ。

５０．　所定の情報処理装置に装着し、前記情報処理装置から供給されたプログラム及び前記プログラムの実行に必要なデータを受信し、前記プログラムを実行する半導体ＩＣの情報処理方法において、

前記半導体ＩＣ固有の第１の鍵を予め記憶している記憶ステップと、

前記記憶ステップで記憶している前記第１の鍵及び前記情報処理装置から供給されたプログラムの属性から、第２の鍵を生成する鍵生成ステップと、

前記プログラムを第３の鍵で復号する第１の復号ステップと、

前記データを第２の鍵で復号する第２の復号ステップと

を含むことを特徴とする情報処理方法。

５１．　所定の情報処理装置に装着し、前記情報処理装置から供給されたプログラム及び前記プログラムの実行に必要なデータを受信し、前記プログラムを実行する半導体ＩＣに、

前記半導体ＩＣ固有の第１の鍵を予め記憶している記憶ステップと、

前記記憶ステップで記憶している前記第１の鍵及び前記情報処理装置から供給されたプログラムの属性から、第２の鍵を生成する鍵

生成ステップと、

前記プログラムを第３の鍵で復号する第１の復号ステップと、

前記データを第２の鍵で復号する第２の復号ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とするプログラム提供媒体。

５２．　半導体ＩＣに実行させるプログラムを供給する情報処理装置及び前記情報処理装置に装着され、前記情報処理装置から供給されたプログラムを受信し、前記プログラムを実行する半導体ＩＣからなる情報処理システムにおいて、

前記情報処理装置は、前記プログラム及び前記プログラムの実行に必要なデータを蓄積する蓄積手段と、前記蓄積手段に対する前記プログラム及び前記データの蓄積又は読み出しを制御する制御手段と、前記プログラムを前記半導体ＩＣから供給された第１の鍵で暗号化する第１の暗号化手段と、前記データを前記半導体ＩＣから供給された第２の鍵で暗号化する第２の暗号化手段と、暗号化された前記プログラム及び前記プログラムの実行に必要なデータを前記半導体ＩＣに送信するとともに、前記第１の鍵及び前記第２の鍵を前記半導体ＩＣから受信する第１の通信手段とを含み、

前記半導体ＩＣは、暗号化された前記プログラム及び前記プログラムの実行に必要なデータを前記情報処理装置から受信するとともに、前記第１の鍵及び前記第２の鍵を前記情報処理装置に送信する第２の通信手段と、前記半導体ＩＣ固有の第３の鍵を予め記憶している記憶手段と、前記記憶手段が記憶している前記第３の鍵及び前記情報処理装置から供給されたプログラムの属性から、第２の鍵を生成する鍵生成手段と、前記第２の通信手段が受信した、前記プロ

グラムを第１の鍵で復号する第１の復号手段と、前記第２の通信手段が受信した、前記データを第２の鍵で復号する第２の復号手段とを含む

ことを特徴とする情報処理システム。

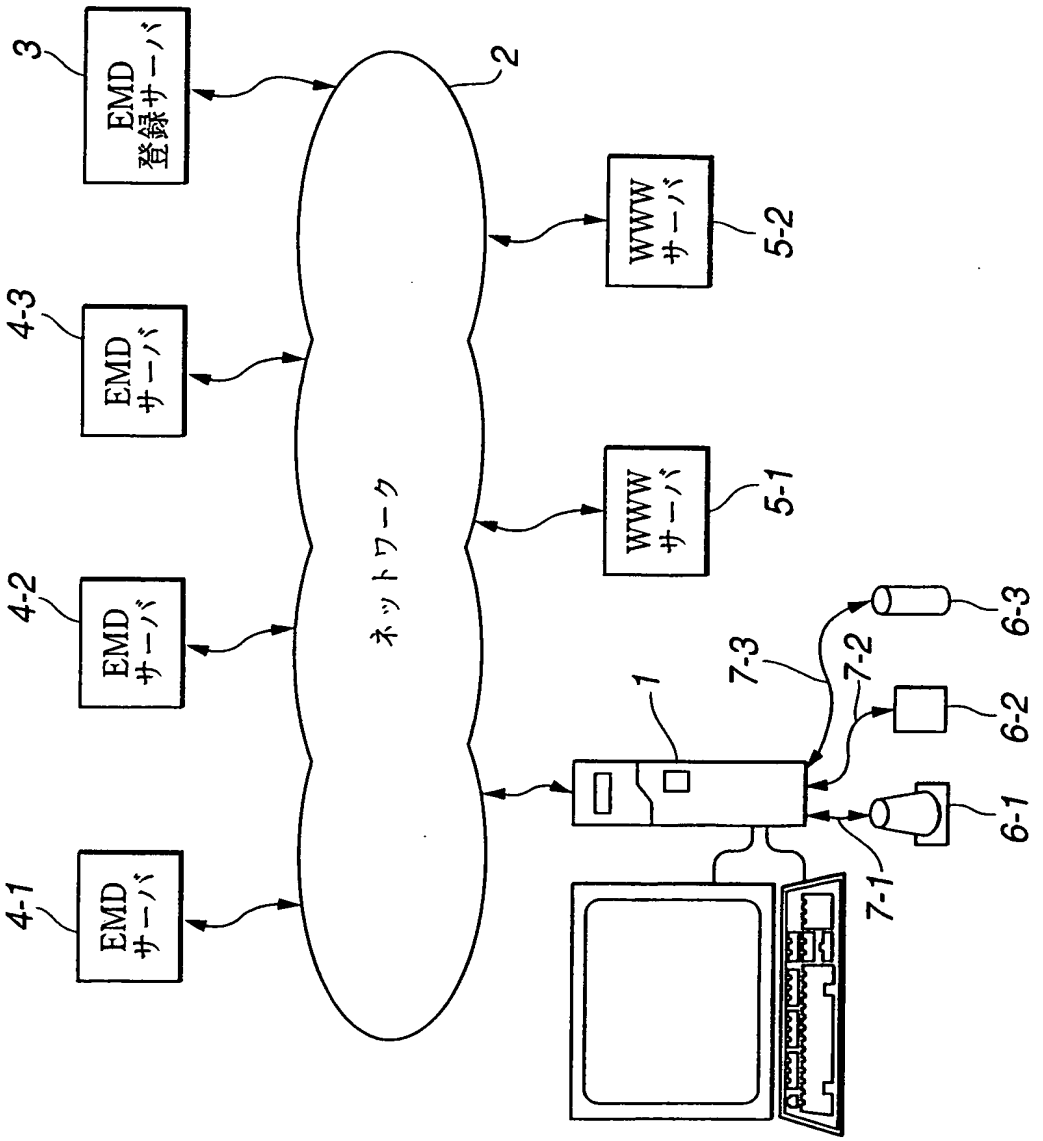

3
EMD
登録サーバ
2
4-3
EMD
サーバ
WWW
サーバ
5-2
4-2
EMD
サーバ
ネットワーク
WWW
サーバ
5-1
4-1
EMD
サーバ
1
7-3
7-2
6-3
6-2
6-1
7-1

FIG.1

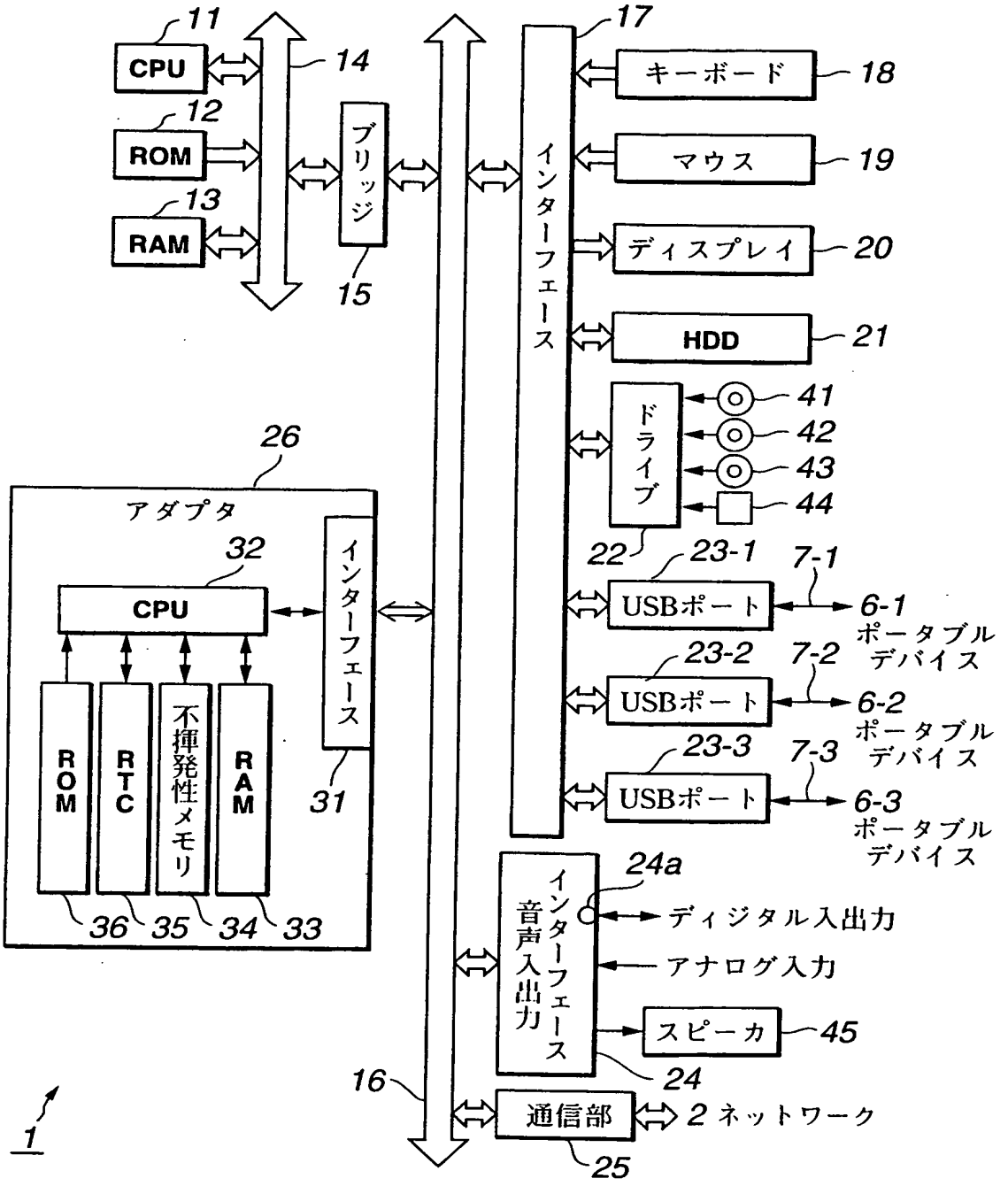

11
CPU
12
ROM
13
RAM
14
ブリッジ
15
17
インターフェース
キーボード
18
マウス
19
ディスプレイ
20
HDD
21
ドライブ
41
42
43
44
22
23-1
USBポート
7-1
6-1
ポータブルデバイス
23-2
USBポート
7-2
6-2
ポータブルデバイス
23-3
USBポート
7-3
6-3
ポータブルデバイス
26
アダプタ
32
CPU
インターフェース
31
ROM
RTC
不揮発性メモリ
RAM
36
35
34
33
24a
インターフェース
音声入出力
ディジタル入出力
アナログ入力
スピーカ
45
24
16
通信部
2 ネットワーク
25
1

FIG.2

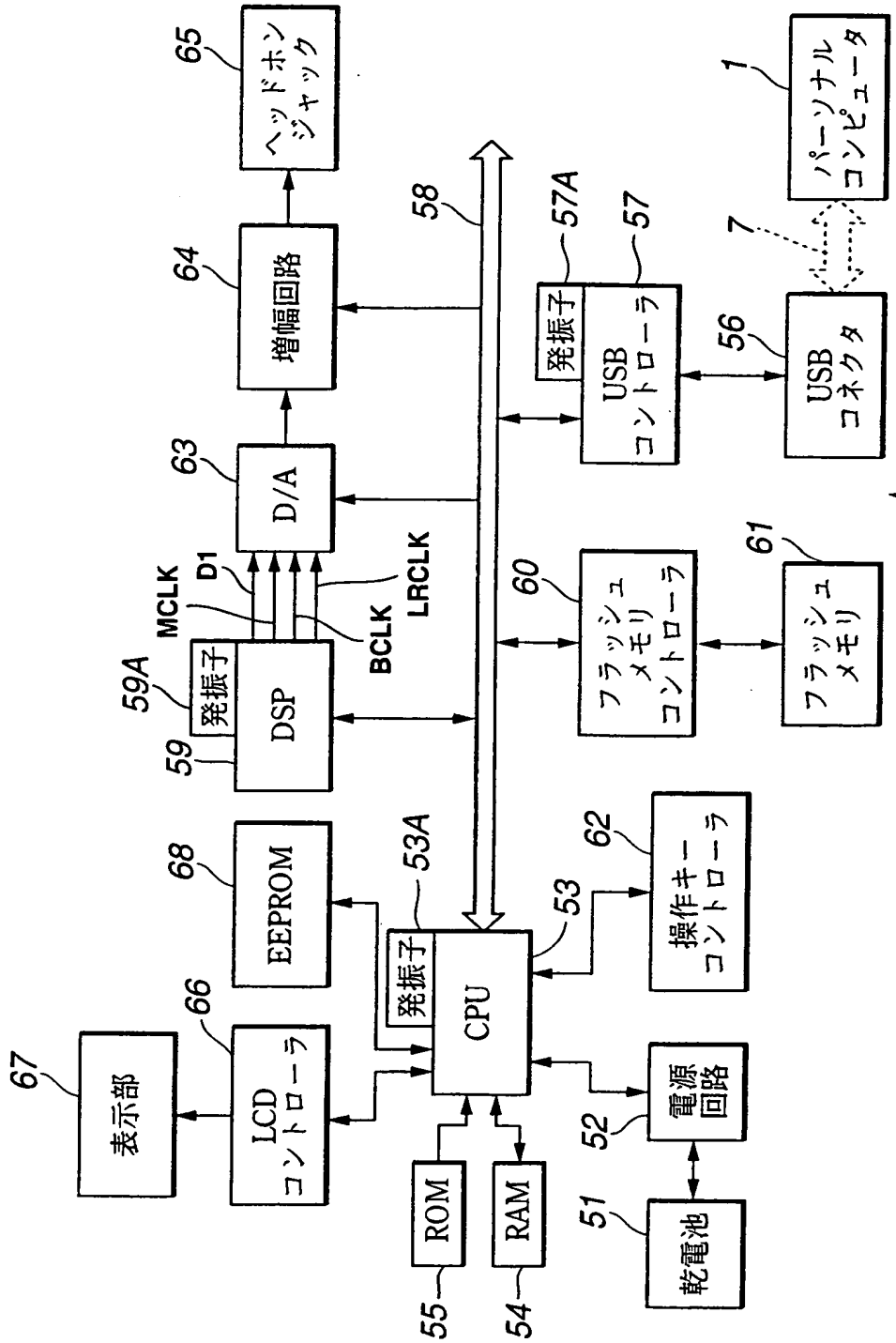

65
ヘッドホン
ジャック
64
増幅回路
63
D/A
MCLK
D1
BCLK
LRCLK
59A
発振子
59
DSP
58
57A
57
発振子
USB
コントローラ
56
USB
コネクタ
7
1
パーソナル
コンピュータ
6
60
フラッシュ
メモリ
コントローラ
61
フラッシュ
メモリ
68
EEPROM
53A
発振子
CPU
53
62
操作キー
コントローラ
66
LCD
コントローラ
67
表示部
ROM
55
RAM
54
52
電源
回路
51
乾電池

FIG.3

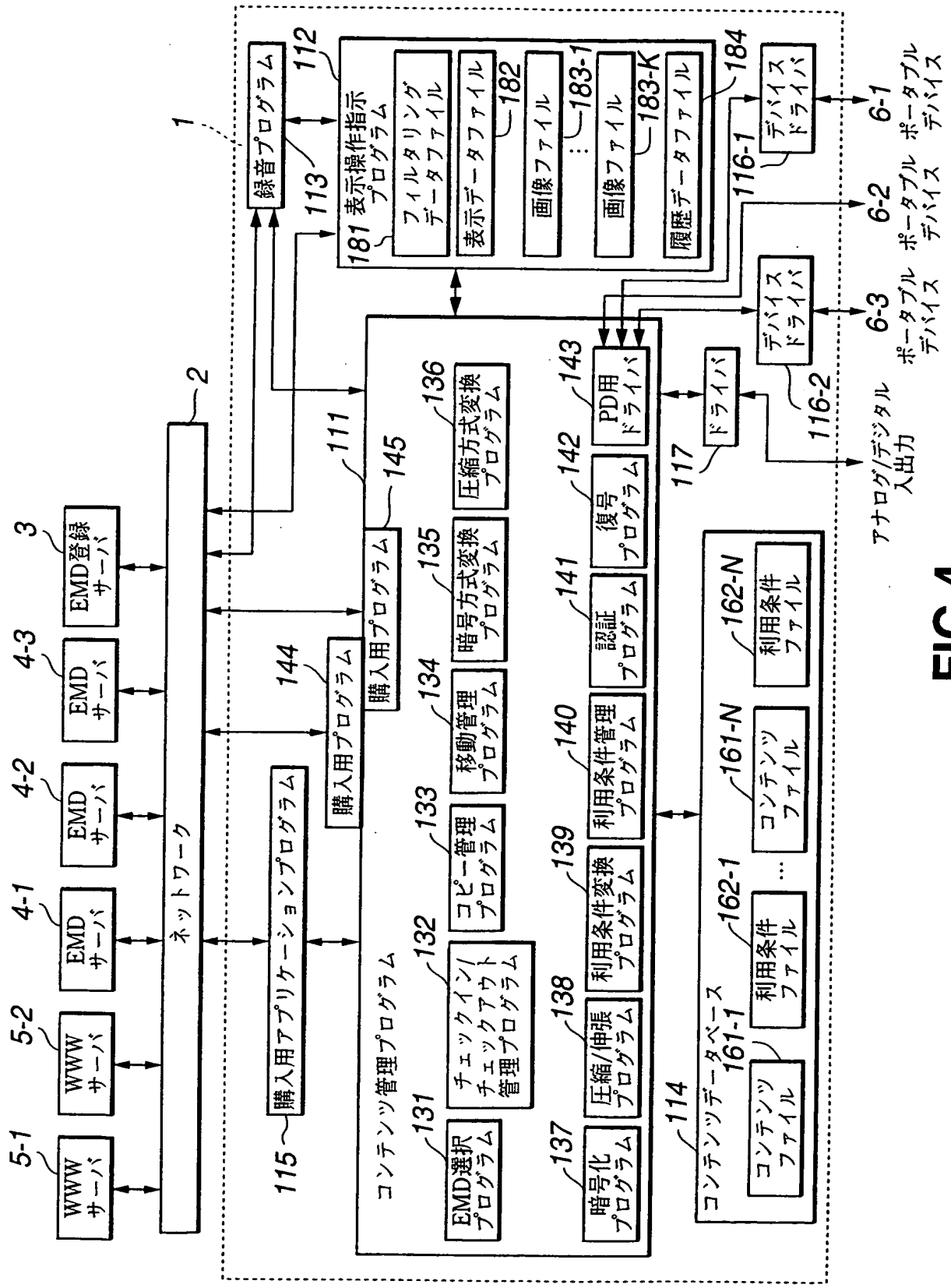

1
2
3
4-1
4-2
4-3
5-1
5-2
6-1
6-2
6-3
111
112
113
114
115
116-1
116-2
117
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
161-1
161-N
162-1
162-N
181
182
183-1
183-K
184
ネットワーク
WWW サーバ
WWW サーバ
EMD サーバ
EMD サーバ
EMD サーバ
EMD登録 サーバ
購入用アプリケーションプログラム
録音プログラム
表示操作指示 プログラム
フィルタリング データファイル
表示データファイル
画像ファイル
画像ファイル
履歴データファイル
デバイス ドライバ
デバイス ドライバ
ドライバ
PD用 ドライバ
購入用プログラム
購入用プログラム
コンテンツ管理プログラム
EMD選択 プログラム
チェックイン/ チェックアウト 管理プログラム
コピー管理 プログラム
移動管理 プログラム
暗号方式変換 プログラム
圧縮方式変換 プログラム
暗号化 プログラム
圧縮/伸張 プログラム
利用条件変換 プログラム
利用条件管理 プログラム
認証 プログラム
復号 プログラム
コンテンツデータベース
コンテンツ ファイル
利用条件 ファイル
コンテンツ ファイル
利用条件 ファイル
アナログ/デジタル 入出力
ポータブル デバイス
ポータブル デバイス

FIG.4

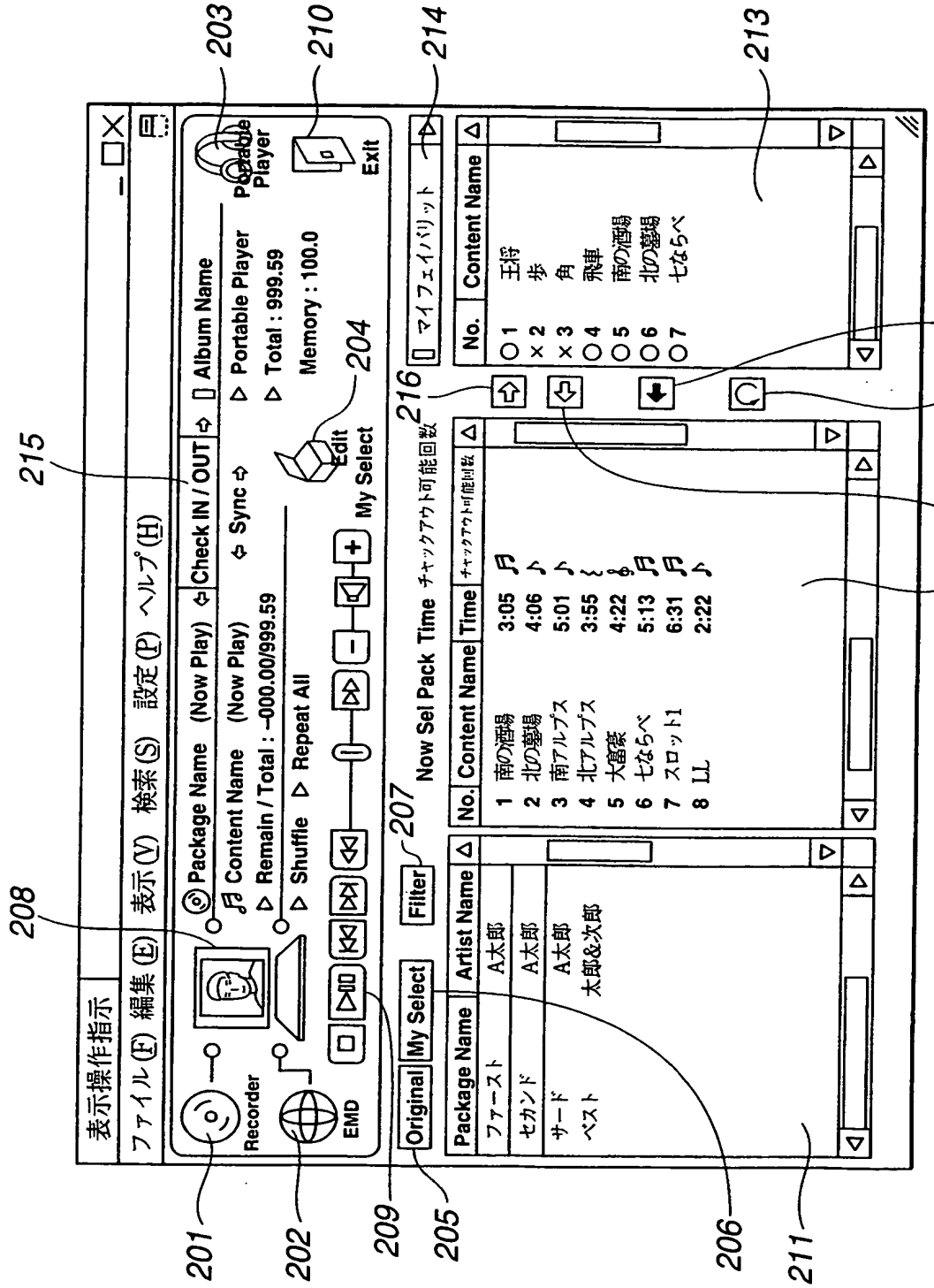

表示操作指示
ファイル(F) 編集(E) 表示(V) 検索(S) 設定(P) ヘルプ(H)
Package Name (Now Play)
Check IN / OUT
Album Name
Content Name (Now Play)
Sync
Portable Player
Total : 999.59
Remain / Total : -000.00/999.59
Memory : 100.0
Shuffle
Repeat All
Edit
My Select
Exit
Recorder
EMD
Original
My Select
Filter
Now Sel Pack Time チャックアウト可能回数
マイフェイバリット
No. Content Name Time チャックアウト可能回数
1 南の酒場 3:05
2 北の墓場 4:06
3 南アルプス 5:01
4 北アルプス 3:55
5 大富豪 4:22
6 七ならべ 5:13
7 スロット1 6:31
8 LL 2:22
No. Content Name
1 王将
2 歩
3 角
4 飛車
5 南の酒場
6 北の墓場
7 七ならべ
Package Name Artist Name
ファースト A太郎
セカンド A太郎
サード A太郎
ベスト 太郎&次郎
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219

FIG.5

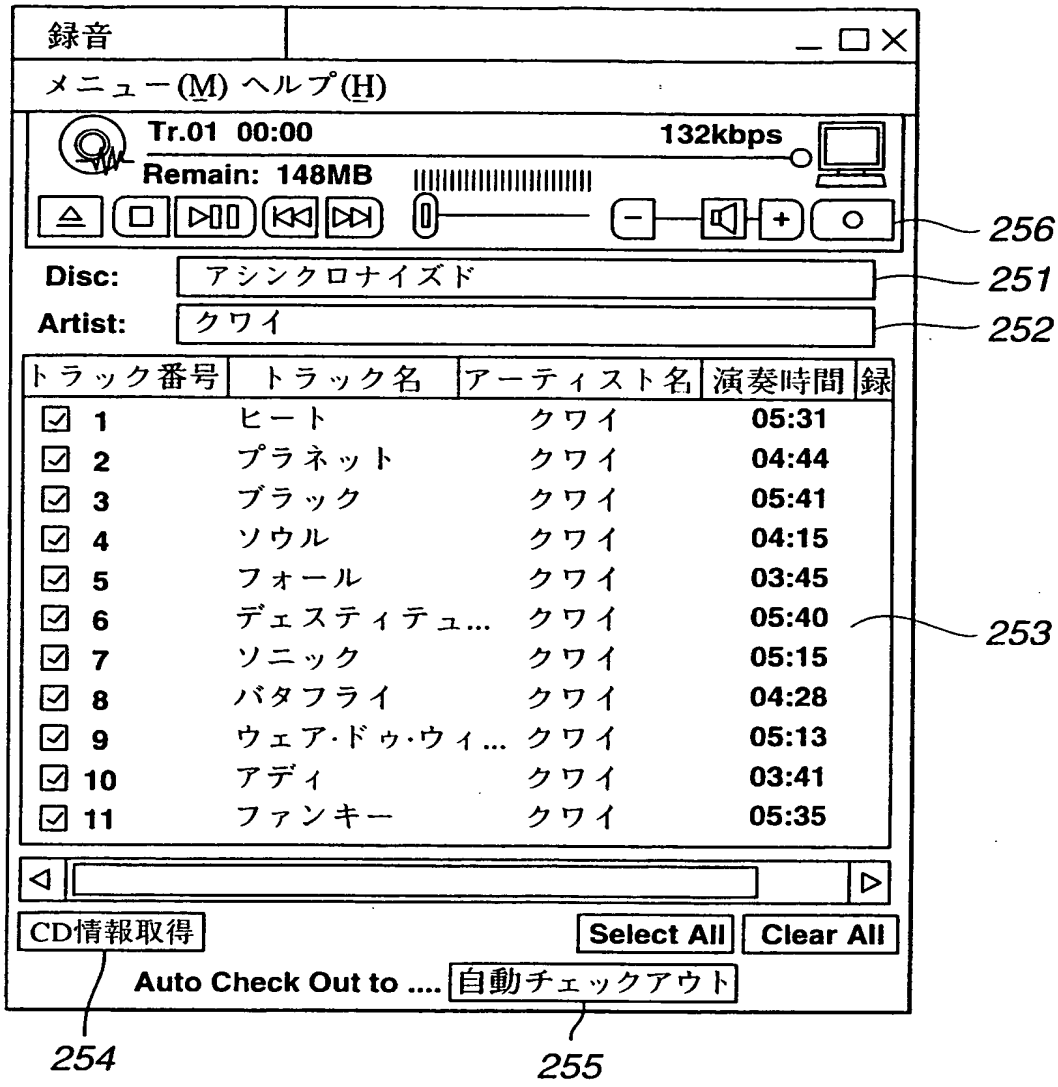

録音
メニュー(M) ヘルプ(H)
Tr.01 00:00
132kbps
Remain: 148MB
Disc: アシンクロナイズド
Artist: クワイ
トラック番号 トラック名 アーティスト名 演奏時間 録
1 ヒート クワイ 05:31
2 プラネット クワイ 04:44
3 ブラック クワイ 05:41
4 ソウル クワイ 04:15
5 フォール クワイ 03:45
6 デェスティテュ... クワイ 05:40
7 ソニック クワイ 05:15
8 バタフライ クワイ 04:28
9 ウェア・ドゥ・ウィ... クワイ 05:13
10 アディ クワイ 03:41
11 ファンキー クワイ 05:35
CD情報取得
Select All
Clear All
Auto Check Out to .... 自動チェックアウト
256
251
252
253
254
255

FIG.6

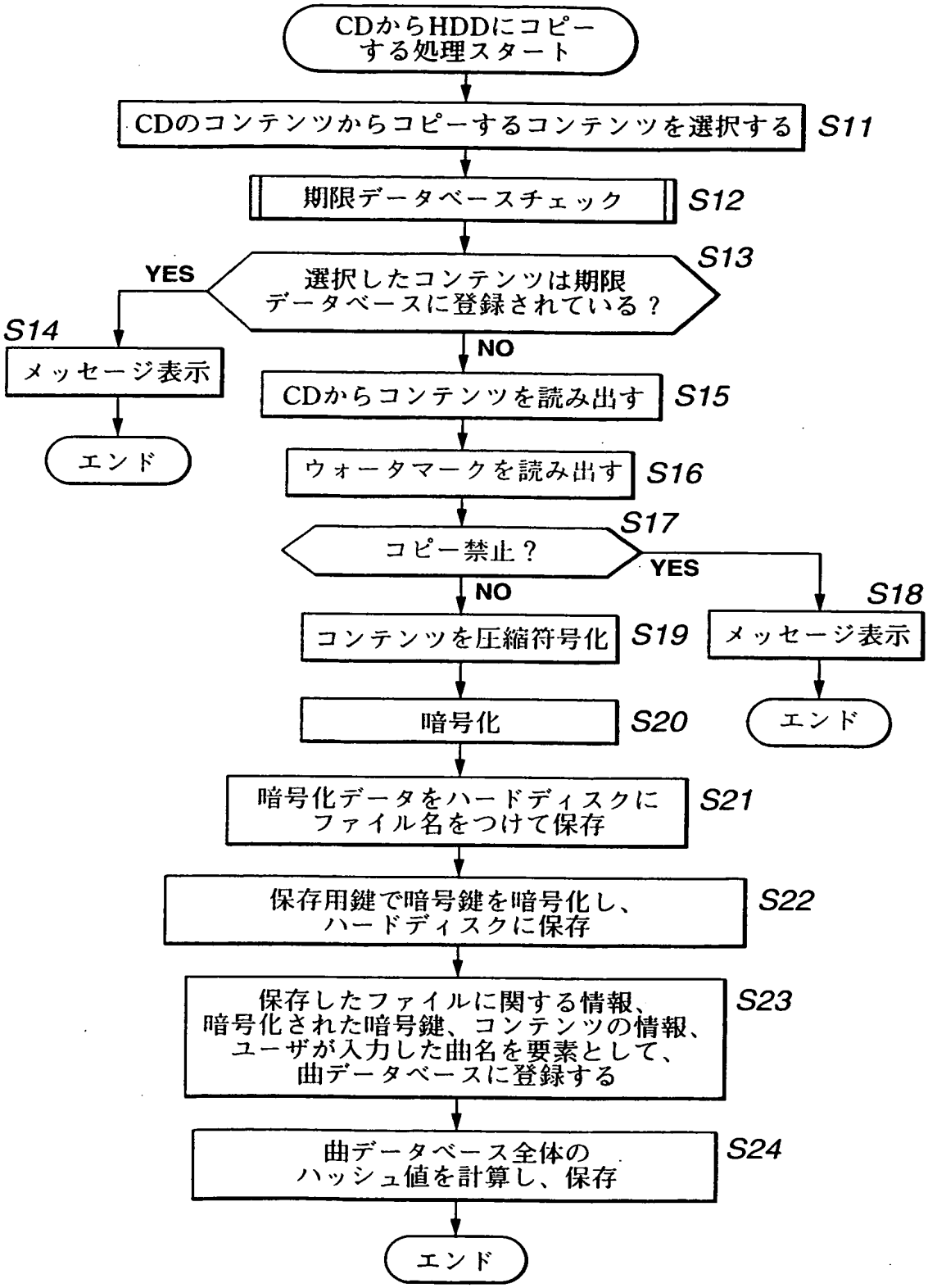

CDからHDDにコピーする処理スタート
CDのコンテンツからコピーするコンテンツを選択する
S11
期限データベースチェック
S12
選択したコンテンツは期限データベースに登録されている？
S13
YES
S14
メッセージ表示
エンド
NO
CDからコンテンツを読み出す
S15
ウォータマークを読み出す
S16
コピー禁止？
S17
YES
S18
メッセージ表示
エンド
NO
コンテンツを圧縮符号化
S19
暗号化
S20
暗号化データをハードディスクにファイル名をつけて保存
S21
保存用鍵で暗号鍵を暗号化し、ハードディスクに保存
S22
保存したファイルに関する情報、暗号化された暗号鍵、コンテンツの情報、ユーザが入力した曲名を要素として、曲データベースに登録する
S23
曲データベース全体のハッシュ値を計算し、保存
S24
エンド

FIG.7

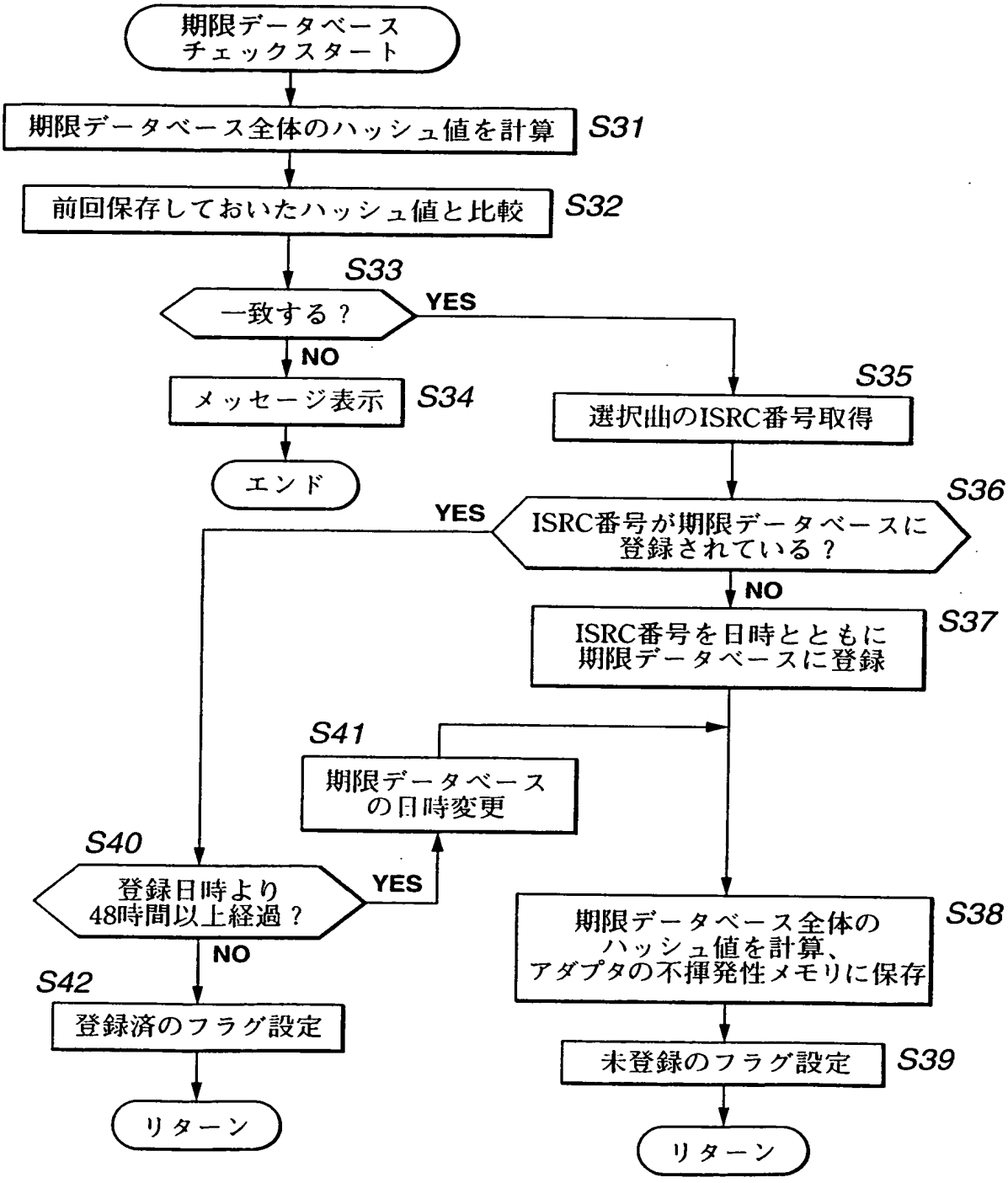

期限データベース
チェックスタート
期限データベース全体のハッシュ値を計算
S31
前回保存しておいたハッシュ値と比較
S32
S33
一致する？
YES
NO
メッセージ表示
S34
エンド
S35
選択曲のISRC番号取得
S36
YES
ISRC番号が期限データベースに
登録されている？
NO
ISRC番号を日時とともに
期限データベースに登録
S37
S41
期限データベース
の日時変更
S40
登録日時より
48時間以上経過？
YES
NO
S42
登録済のフラグ設定
リターン
期限データベース全体の
ハッシュ値を計算、
アダプタの不揮発性メモリに保存
S38
未登録のフラグ設定
S39
リターン

FIG.8

	アイテム1	アイテム2	アイテム3	
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347	
コピー日時	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16.15	

ハッシュ値	0xf3352e125934

FIG.9

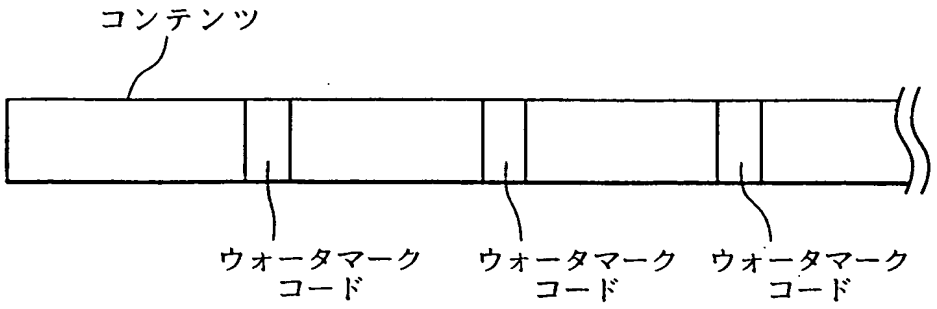


FIG.10

	アイテム1	アイテム2	アイテム3	
ファイル名	Xd000110. at2	px92341234. at2	aa0234287034. at2	
暗号化された暗号鍵	0xabababababab	0x9898989898989	0x123456789012	
曲名	春の小川	運命	荒城の月	
長さ	180	190	200	
再生条件 : 開始日時	-	2001.01.01.00:00	-	
再生条件 : 終了日時	1999.07.31.23:59	-	-	
再生条件 : 回数制限	-	20	-	
再生回数カウンタ	-	12	-	
再生時課金条件	-	-	￥5	
コピー条件 : 回数	2	0	0	
コピー回数カウンタ	1	0	0	
コピー条件 : SCMS	0b01	0b10	0b00	

ハッシュ値	0xf9951e566321

FIG.11

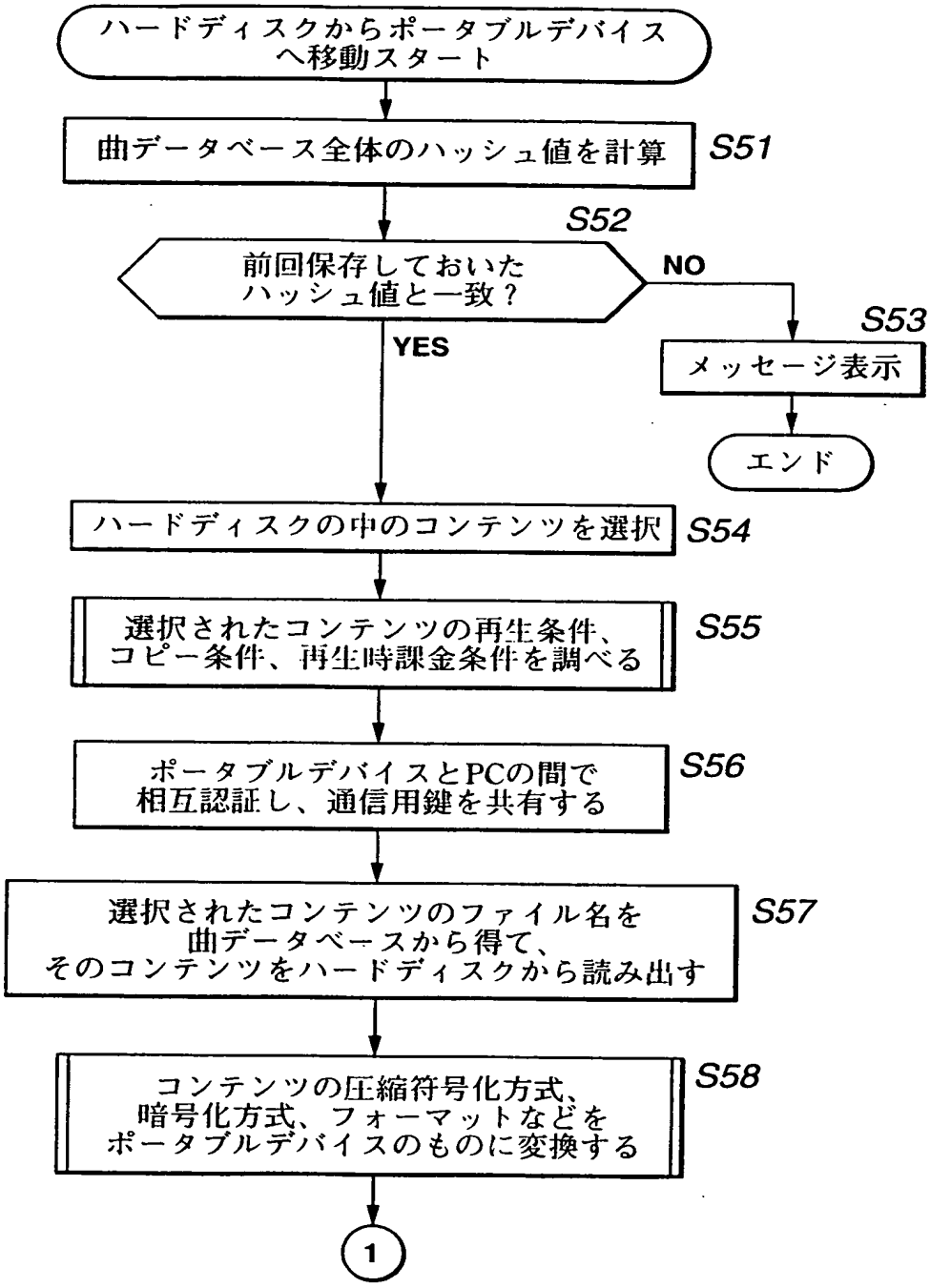

ハードディスクからポータブルデバイスへ移動スタート
曲データベース全体のハッシュ値を計算
S51
S52
前回保存しておいたハッシュ値と一致？
NO
YES
S53
メッセージ表示
エンド
ハードディスクの中のコンテンツを選択
S54
選択されたコンテンツの再生条件、コピー条件、再生時課金条件を調べる
S55
ポータブルデバイスとPCの間で相互認証し、通信用鍵を共有する
S56
選択されたコンテンツのファイル名を曲データベースから得て、そのコンテンツをハードディスクから読み出す
S57
コンテンツの圧縮符号化方式、暗号化方式、フォーマットなどをポータブルデバイスのものに変換する
S58
1

FIG.12

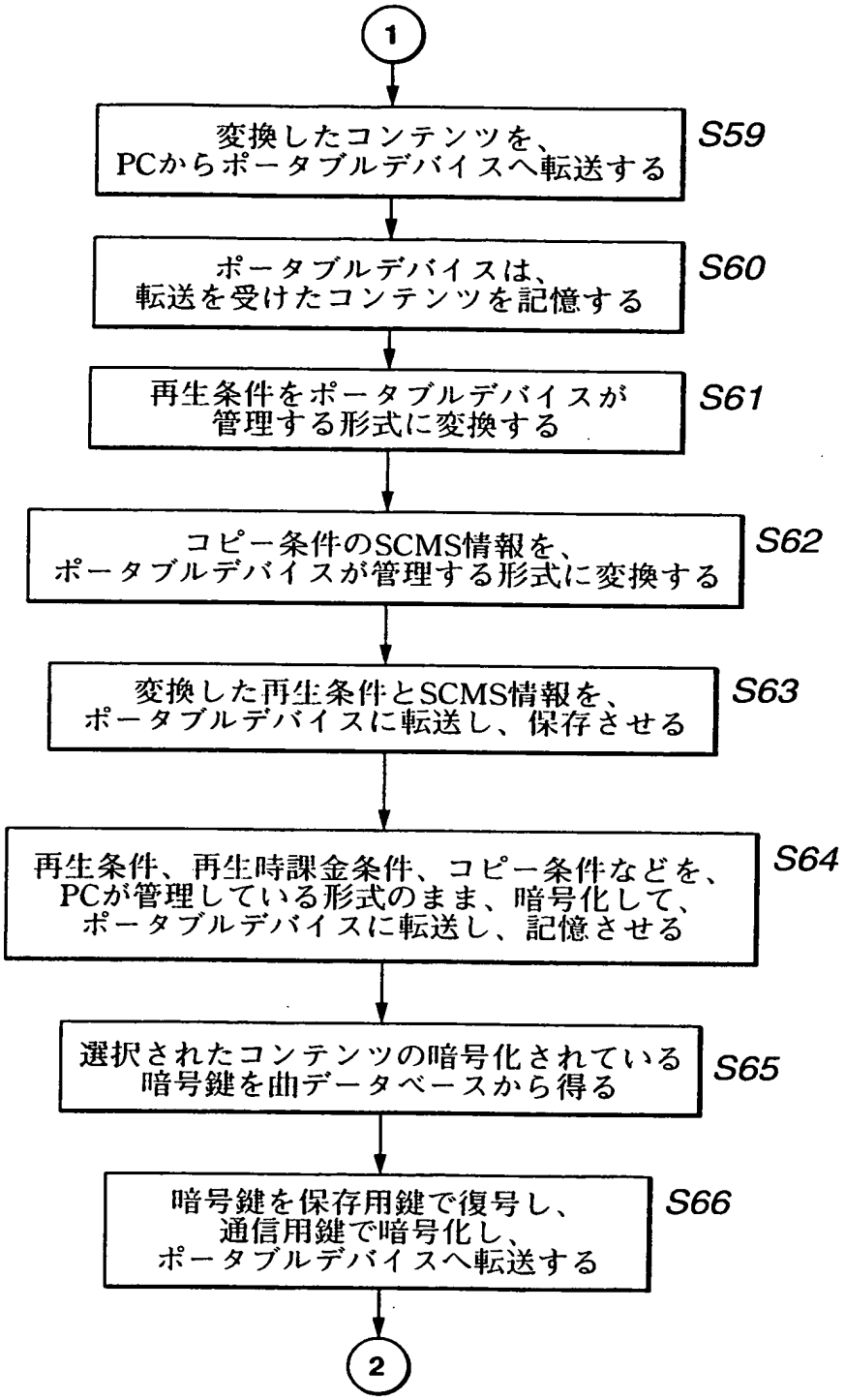

1
変換したコンテンツを、
PCからポータブルデバイスへ転送する
S59
ポータブルデバイスは、
転送を受けたコンテンツを記憶する
S60
再生条件をポータブルデバイスが
管理する形式に変換する
S61
コピー条件のSCMS情報を、
ポータブルデバイスが管理する形式に変換する
S62
変換した再生条件とSCMS情報を、
ポータブルデバイスに転送し、保存させる
S63
再生条件、再生時課金条件、コピー条件などを、
PCが管理している形式のまま、暗号化して、
ポータブルデバイスに転送し、記憶させる
S64
選択されたコンテンツの暗号化されている
暗号鍵を曲データベースから得る
S65
暗号鍵を保存用鍵で復号し、
通信用鍵で暗号化し、
ポータブルデバイスへ転送する
S66
2

FIG.13

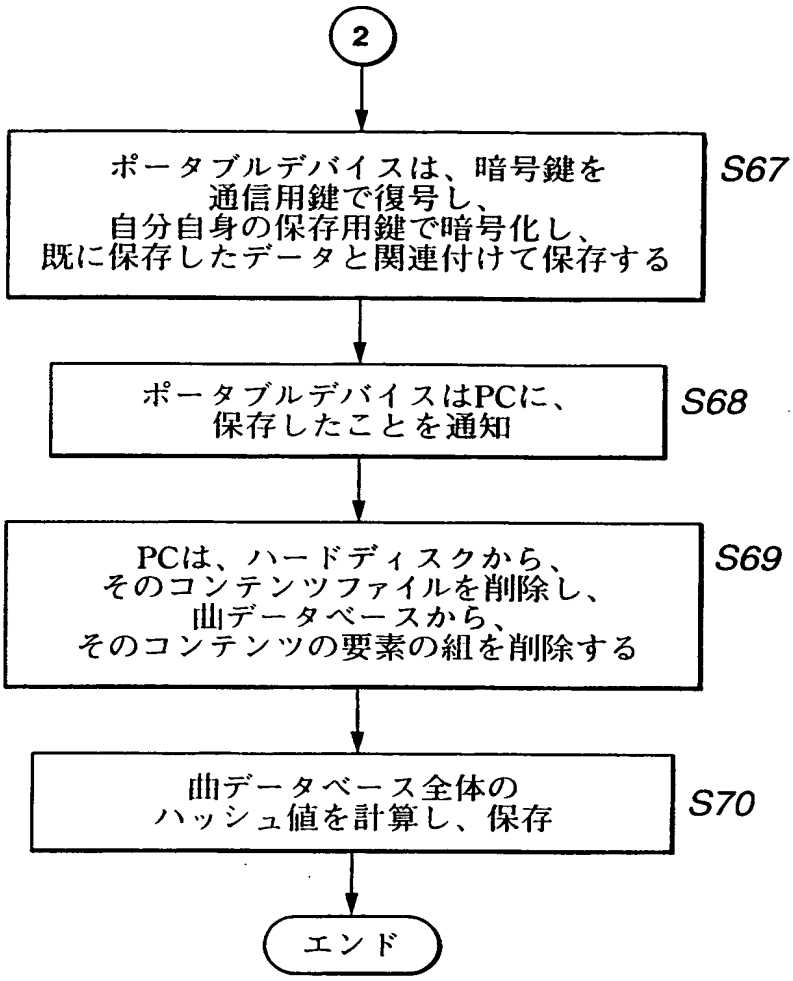

2
ポータブルデバイスは、暗号鍵を
通信用鍵で復号し、
自分自身の保存用鍵で暗号化し、
既に保存したデータと関連付けて保存する
S67
ポータブルデバイスはPCに、
保存したことを通知
S68
PCは、ハードディスクから、
そのコンテンツファイルを削除し、
曲データベースから、
そのコンテンツの要素の組を削除する
S69
曲データベース全体の
ハッシュ値を計算し、保存
S70
エンド

FIG.14

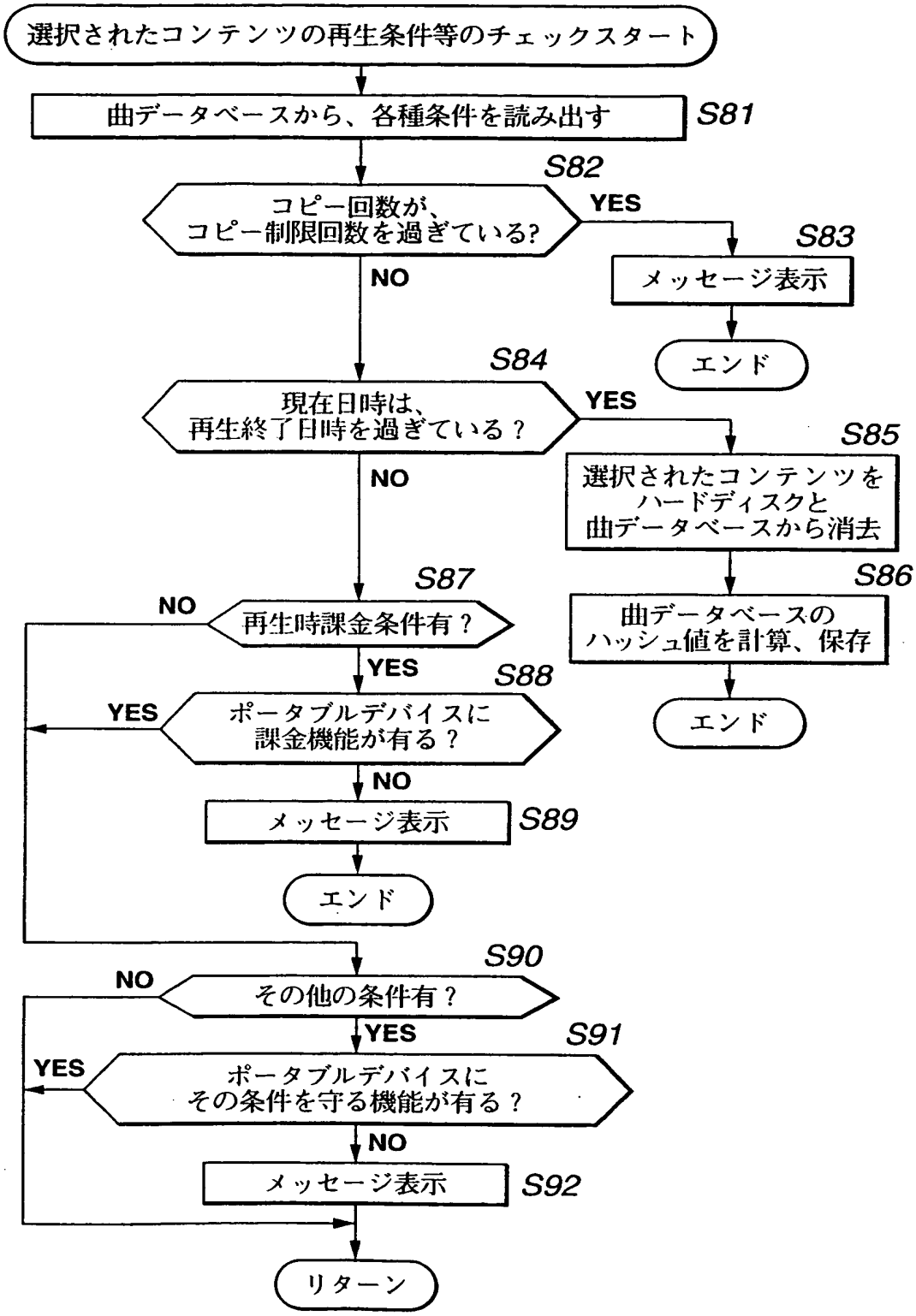

選択されたコンテンツの再生条件等のチェックスタート
曲データベースから、各種条件を読み出す
S81
S82
コピー回数が、
コピー制限回数を過ぎている?
YES
S83
メッセージ表示
エンド
NO
S84
現在日時は、
再生終了日時を過ぎている？
YES
S85
選択されたコンテンツを
ハードディスクと
曲データベースから消去
S86
曲データベースの
ハッシュ値を計算、保存
エンド
NO
S87
再生時課金条件有？
NO
YES
S88
ポータブルデバイスに
課金機能が有る？
YES
NO
メッセージ表示
S89
エンド
S90
その他の条件有？
NO
YES
S91
ポータブルデバイスに
その条件を守る機能が有る？
YES
NO
メッセージ表示
S92
リターン

FIG.15

	アイテム1	アイテム2	アイテム3
コンテンツID	00001	00002	00003
再生開始日時	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
再生終了日時	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
再生回数	-	15	-

FIG.16

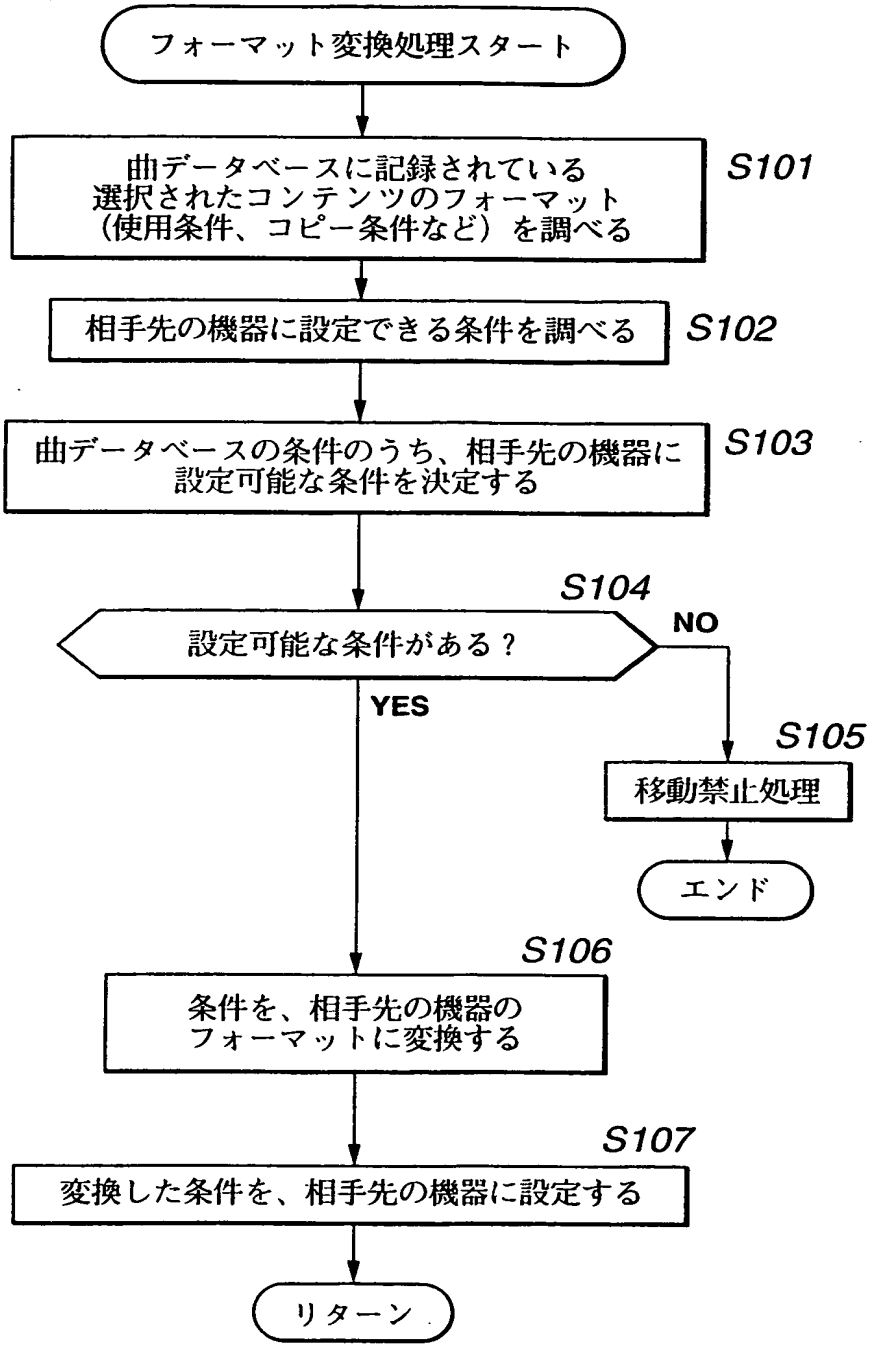

フォーマット変換処理スタート
曲データベースに記録されている
選択されたコンテンツのフォーマット
（使用条件、コピー条件など）を調べる
S101
相手先の機器に設定できる条件を調べる
S102
曲データベースの条件のうち、相手先の機器に
設定可能な条件を決定する
S103
S104
設定可能な条件がある？
NO
YES
S105
移動禁止処理
エンド
S106
条件を、相手先の機器の
フォーマットに変換する
S107
変換した条件を、相手先の機器に設定する
リターン

FIG.17

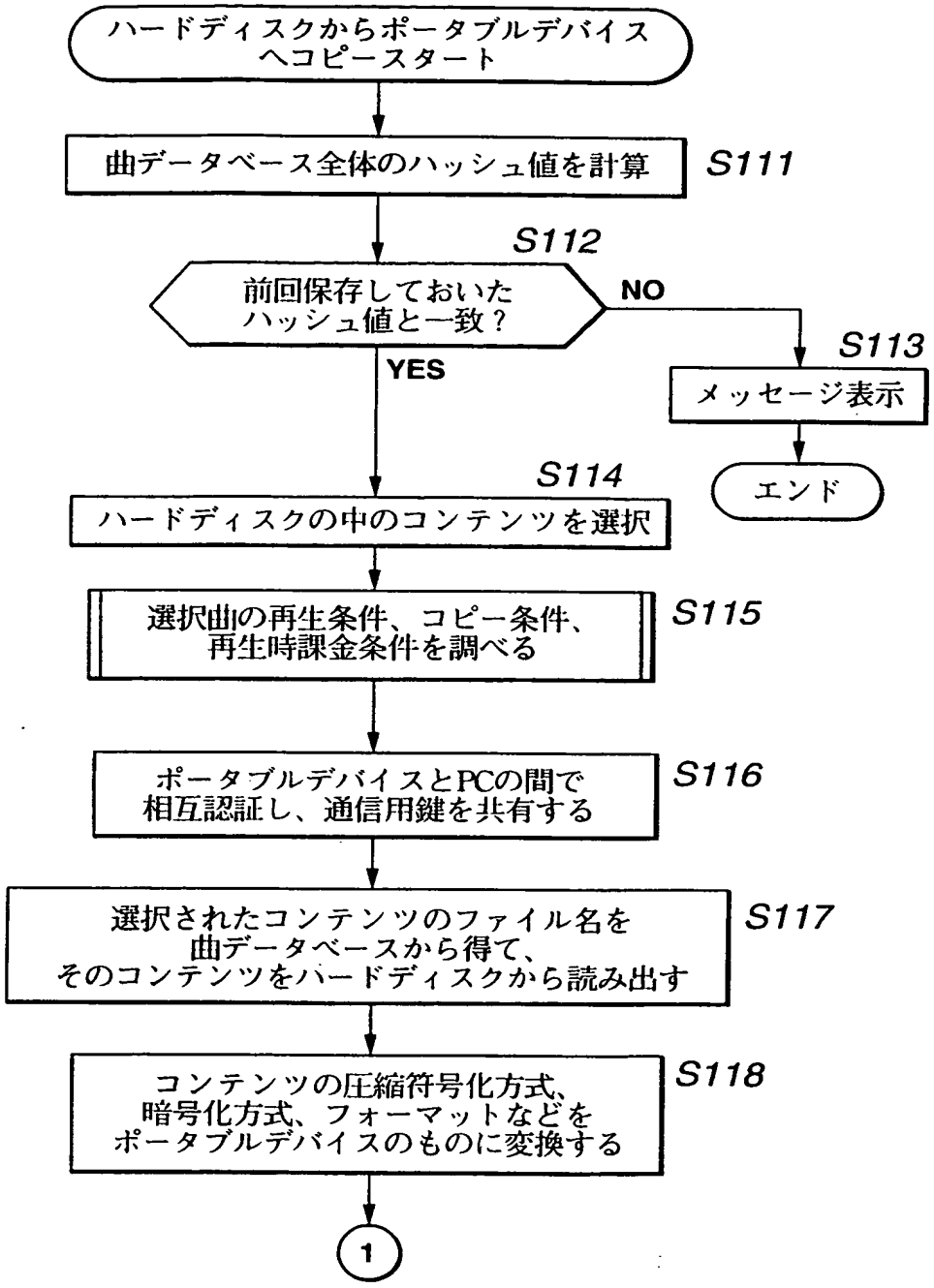

ハードディスクからポータブルデバイスへコピースタート
曲データベース全体のハッシュ値を計算
S111
S112
前回保存しておいたハッシュ値と一致？
NO
YES
S113
メッセージ表示
エンド
S114
ハードディスクの中のコンテンツを選択
選択曲の再生条件、コピー条件、再生時課金条件を調べる
S115
ポータブルデバイスとPCの間で相互認証し、通信用鍵を共有する
S116
選択されたコンテンツのファイル名を曲データベースから得て、そのコンテンツをハードディスクから読み出す
S117
コンテンツの圧縮符号化方式、暗号化方式、フォーマットなどをポータブルデバイスのものに変換する
S118
1

FIG.18

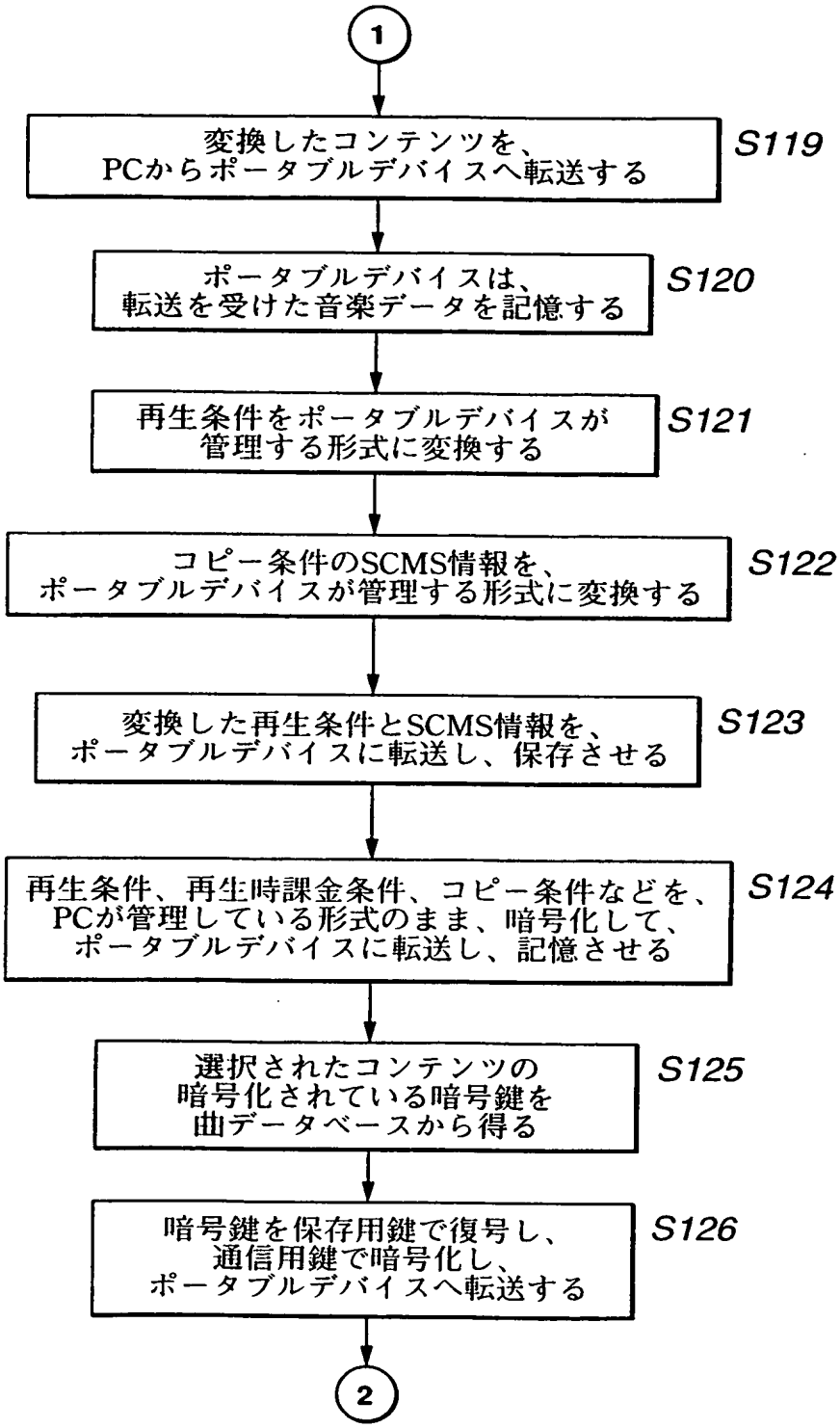

1
変換したコンテンツを、
PCからポータブルデバイスへ転送する
S119
ポータブルデバイスは、
転送を受けた音楽データを記憶する
S120
再生条件をポータブルデバイスが
管理する形式に変換する
S121
コピー条件のSCMS情報を、
ポータブルデバイスが管理する形式に変換する
S122
変換した再生条件とSCMS情報を、
ポータブルデバイスに転送し、保存させる
S123
再生条件、再生時課金条件、コピー条件などを、
PCが管理している形式のまま、暗号化して、
ポータブルデバイスに転送し、記憶させる
S124
選択されたコンテンツの
暗号化されている暗号鍵を
曲データベースから得る
S125
暗号鍵を保存用鍵で復号し、
通信用鍵で暗号化し、
ポータブルデバイスへ転送する
S126
2

FIG.19

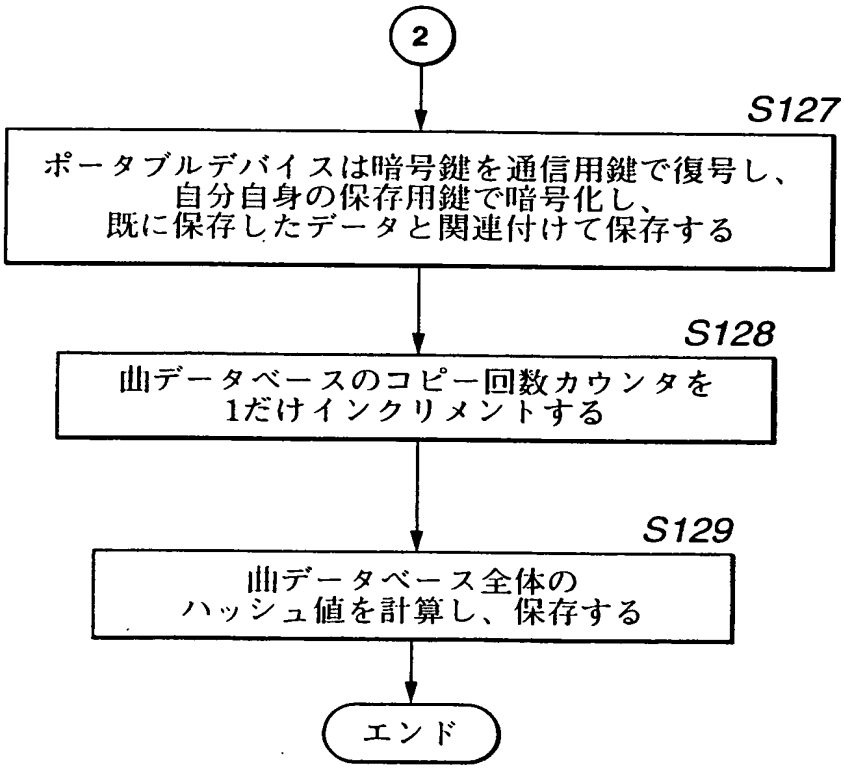

2
S127
ポータブルデバイスは暗号鍵を通信用鍵で復号し、
自分自身の保存用鍵で暗号化し、
既に保存したデータと関連付けて保存する
S128
曲データベースのコピー回数カウンタを
1だけインクリメントする
S129
曲データベース全体の
ハッシュ値を計算し、保存する
エンド

FIG.20

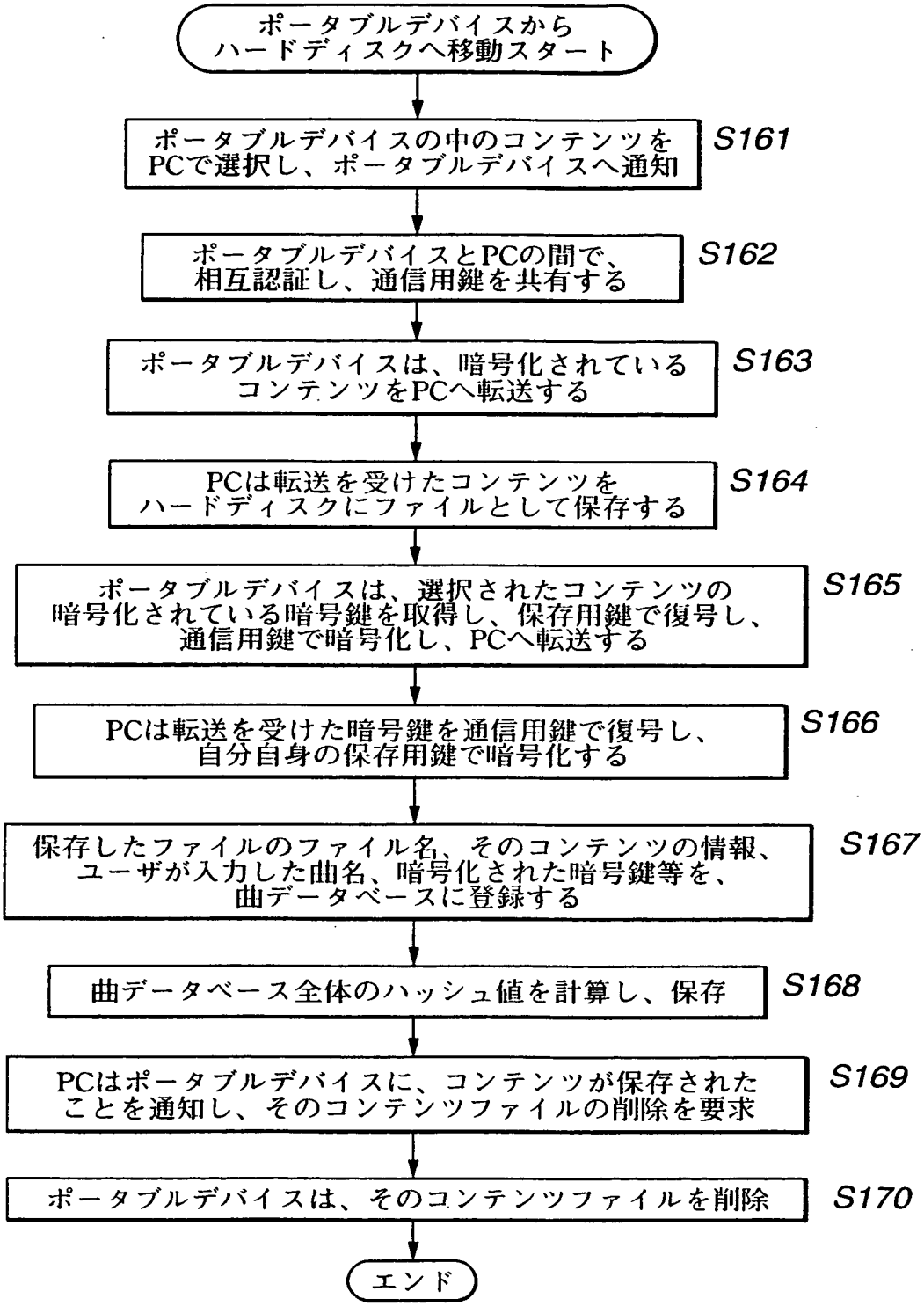

ポータブルデバイスから
ハードディスクへ移動スタート
ポータブルデバイスの中のコンテンツを
PCで選択し、ポータブルデバイスへ通知
S161
ポータブルデバイスとPCの間で、
相互認証し、通信用鍵を共有する
S162
ポータブルデバイスは、暗号化されている
コンテンツをPCへ転送する
S163
PCは転送を受けたコンテンツを
ハードディスクにファイルとして保存する
S164
ポータブルデバイスは、選択されたコンテンツの
暗号化されている暗号鍵を取得し、保存用鍵で復号し、
通信用鍵で暗号化し、PCへ転送する
S165
PCは転送を受けた暗号鍵を通信用鍵で復号し、
自分自身の保存用鍵で暗号化する
S166
保存したファイルのファイル名、そのコンテンツの情報、
ユーザが入力した曲名、暗号化された暗号鍵等を、
曲データベースに登録する
S167
曲データベース全体のハッシュ値を計算し、保存
S168
PCはポータブルデバイスに、コンテンツが保存された
ことを通知し、そのコンテンツファイルの削除を要求
S169
ポータブルデバイスは、そのコンテンツファイルを削除
S170
エンド

FIG.21

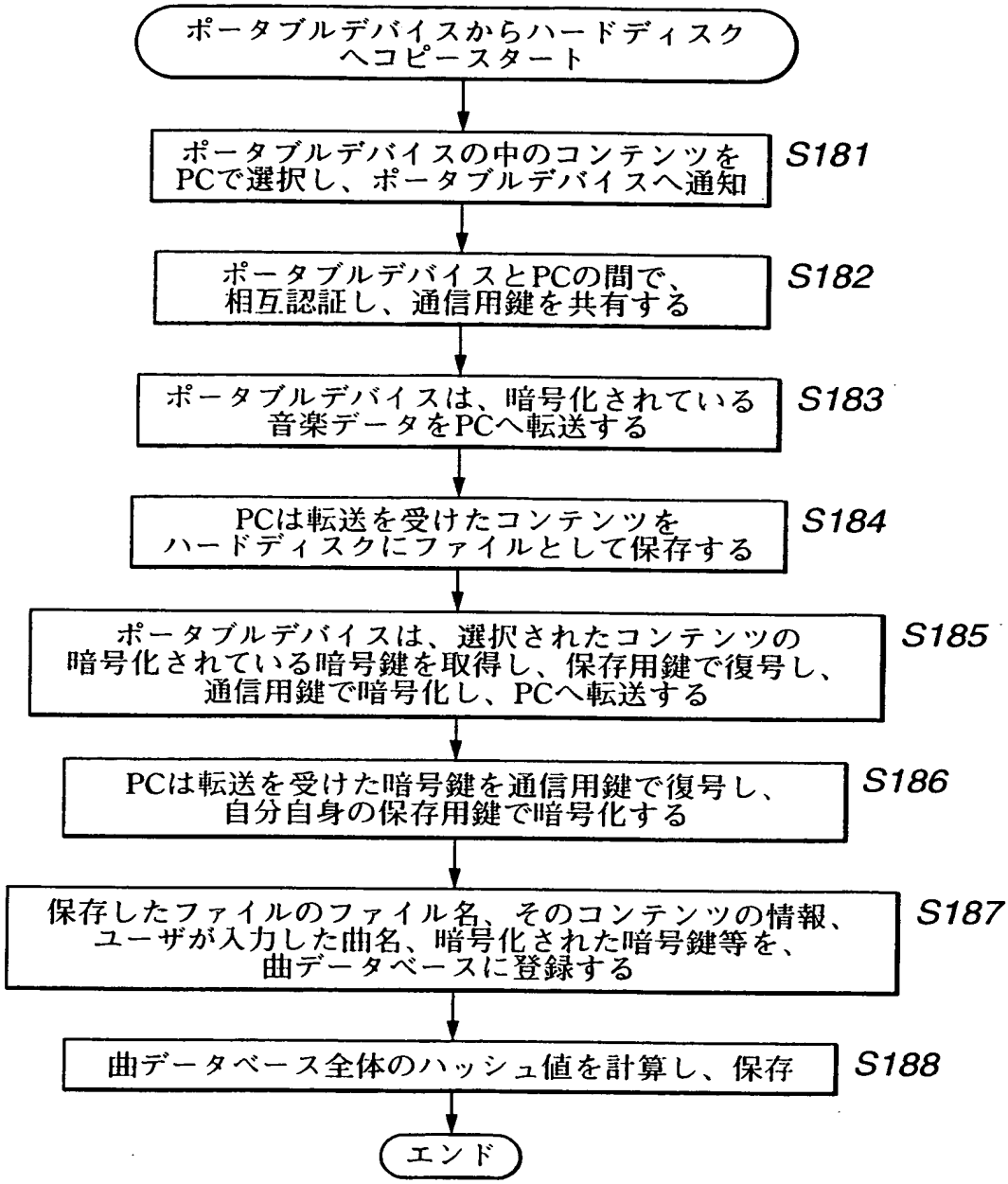

ポータブルデバイスからハードディスクへコピースタート
ポータブルデバイスの中のコンテンツをPCで選択し、ポータブルデバイスへ通知
S181
ポータブルデバイスとPCの間で、相互認証し、通信用鍵を共有する
S182
ポータブルデバイスは、暗号化されている音楽データをPCへ転送する
S183
PCは転送を受けたコンテンツをハードディスクにファイルとして保存する
S184
ポータブルデバイスは、選択されたコンテンツの暗号化されている暗号鍵を取得し、保存用鍵で復号し、通信用鍵で暗号化し、PCへ転送する
S185
PCは転送を受けた暗号鍵を通信用鍵で復号し、自分自身の保存用鍵で暗号化する
S186
保存したファイルのファイル名、そのコンテンツの情報、ユーザが入力した曲名、暗号化された暗号鍵等を、曲データベースに登録する
S187
曲データベース全体のハッシュ値を計算し、保存
S188
エンド

FIG.22

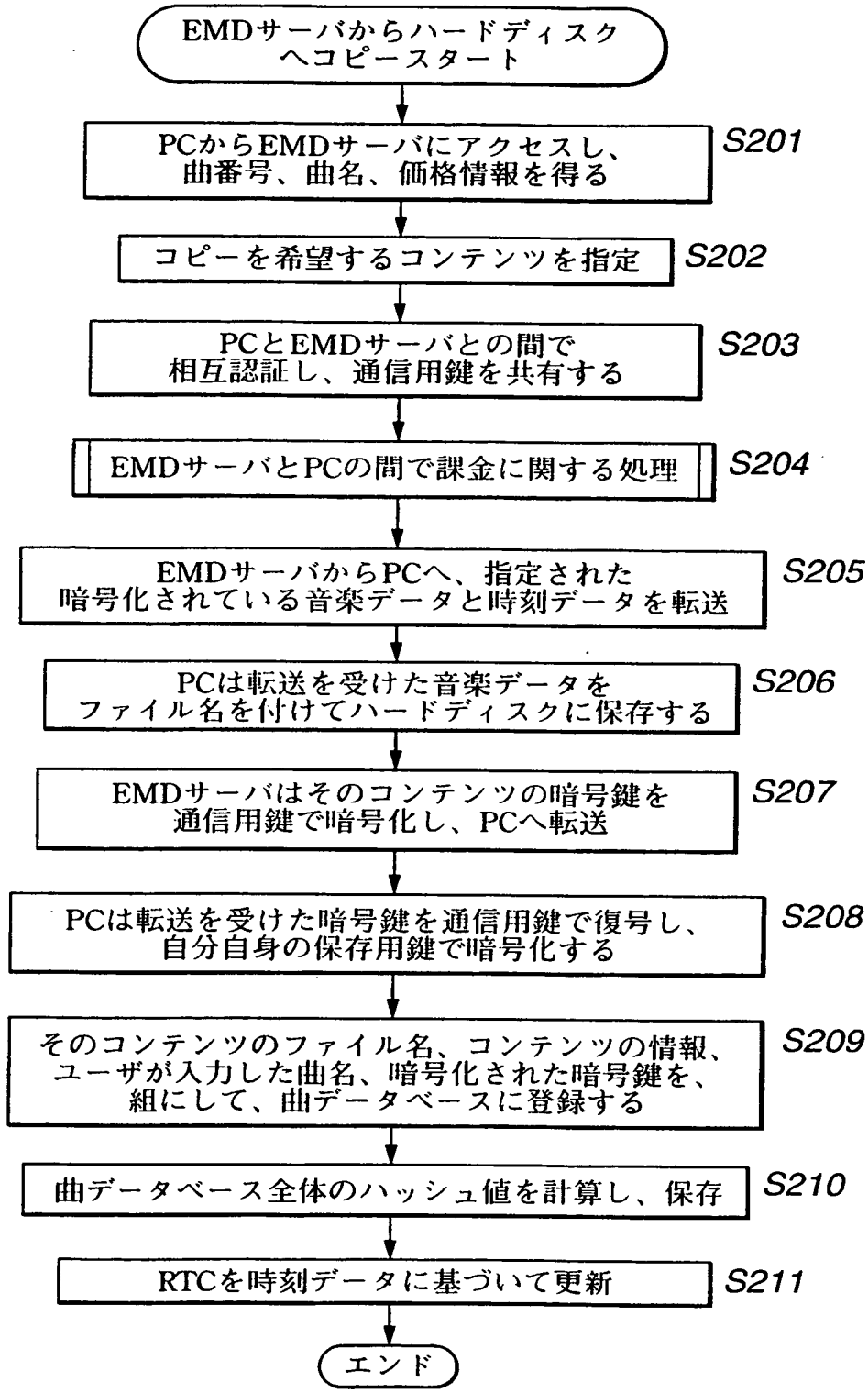

EMDサーバからハードディスクへコピースタート
PCからEMDサーバにアクセスし、曲番号、曲名、価格情報を得る
S201
コピーを希望するコンテンツを指定
S202
PCとEMDサーバとの間で相互認証し、通信用鍵を共有する
S203
EMDサーバとPCの間で課金に関する処理
S204
EMDサーバからPCへ、指定された暗号化されている音楽データと時刻データを転送
S205
PCは転送を受けた音楽データをファイル名を付けてハードディスクに保存する
S206
EMDサーバはそのコンテンツの暗号鍵を通信用鍵で暗号化し、PCへ転送
S207
PCは転送を受けた暗号鍵を通信用鍵で復号し、自分自身の保存用鍵で暗号化する
S208
そのコンテンツのファイル名、コンテンツの情報、ユーザが入力した曲名、暗号化された暗号鍵を、組にして、曲データベースに登録する
S209
曲データベース全体のハッシュ値を計算し、保存
S210
RTCを時刻データに基づいて更新
S211
エンド

FIG.23

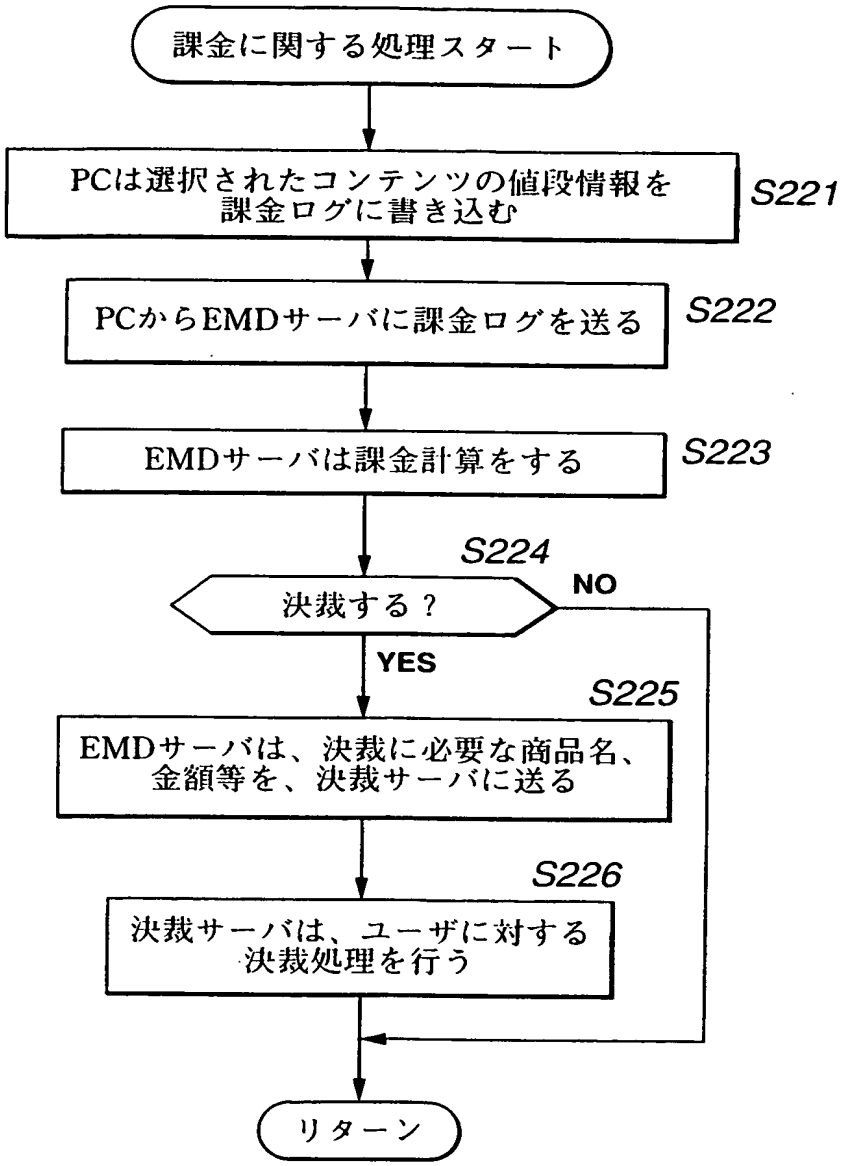

課金に関する処理スタート
PCは選択されたコンテンツの値段情報を課金ログに書き込む
S221
PCからEMDサーバに課金ログを送る
S222
EMDサーバは課金計算をする
S223
S224
決裁する？
NO
YES
S225
EMDサーバは、決裁に必要な商品名、金額等を、決裁サーバに送る
S226
決裁サーバは、ユーザに対する決裁処理を行う
リターン

FIG.24

	アイテム1	アイテム2	アイテム3	
料金	50	50	60	

ハッシュ値	0xf8783e263517

FIG.25

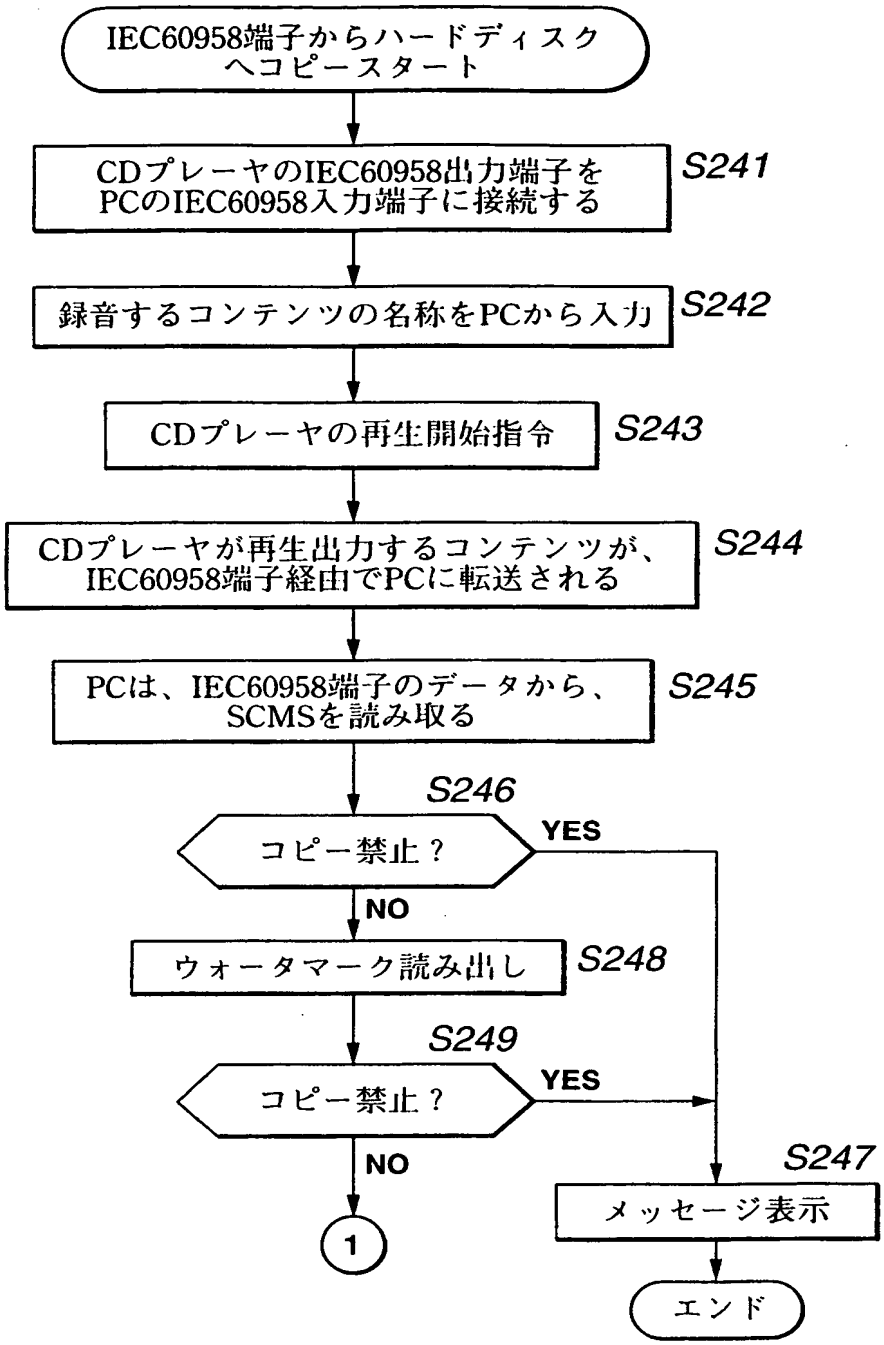

IEC60958端子からハードディスクへコピースタート
CDプレーヤのIEC60958出力端子をPCのIEC60958入力端子に接続する
S241
録音するコンテンツの名称をPCから入力
S242
CDプレーヤの再生開始指令
S243
CDプレーヤが再生出力するコンテンツが、IEC60958端子経由でPCに転送される
S244
PCは、IEC60958端子のデータから、SCMSを読み取る
S245
S246
コピー禁止？
YES
NO
ウォータマーク読み出し
S248
S249
コピー禁止？
YES
NO
S247
メッセージ表示
1
エンド

FIG.26

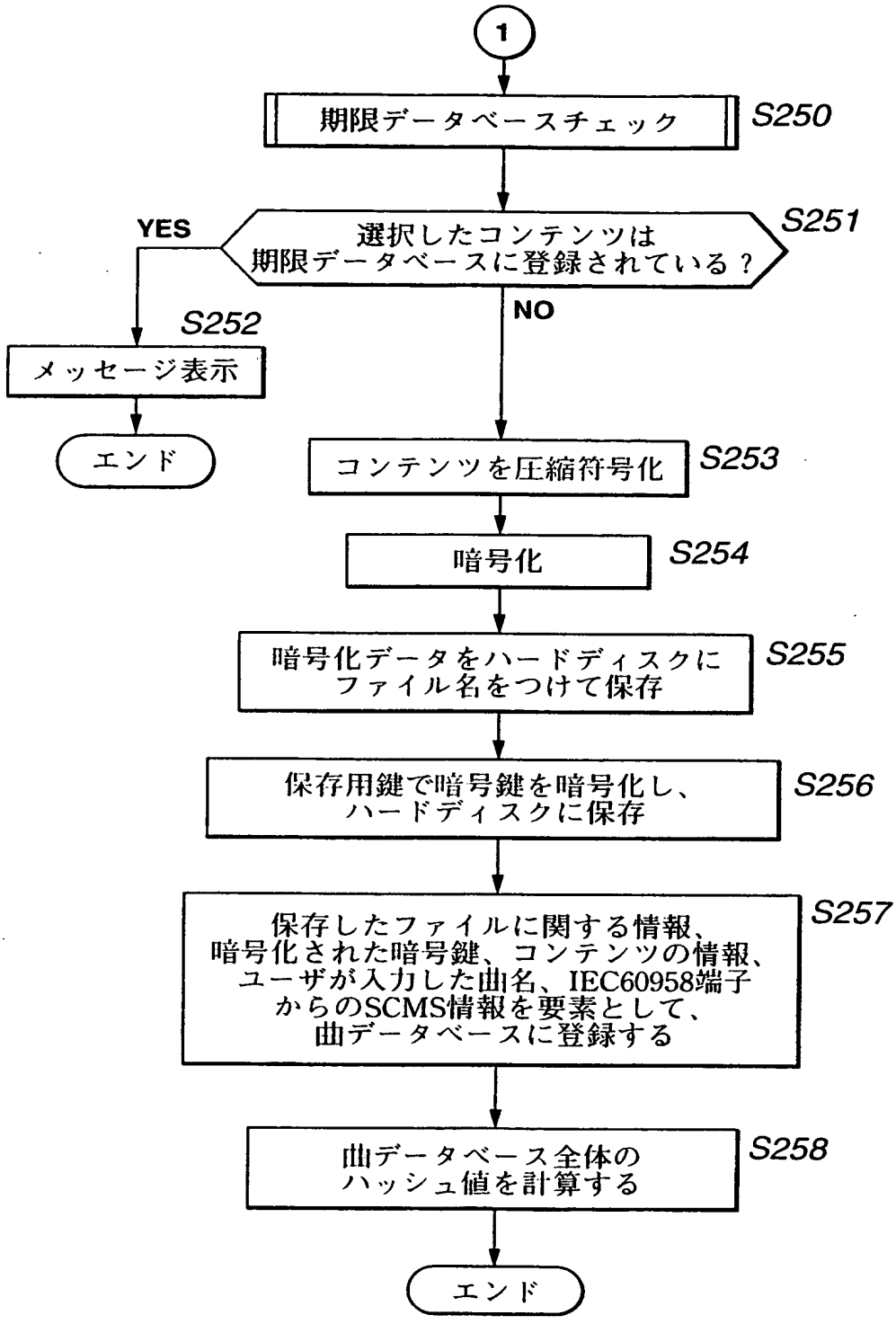

1
期限データベースチェック
S250
選択したコンテンツは
期限データベースに登録されている？
S251
YES
NO
S252
メッセージ表示
エンド
コンテンツを圧縮符号化
S253
暗号化
S254
暗号化データをハードディスクに
ファイル名をつけて保存
S255
保存用鍵で暗号鍵を暗号化し、
ハードディスクに保存
S256
保存したファイルに関する情報、
暗号化された暗号鍵、コンテンツの情報、
ユーザが入力した曲名、IEC60958端子
からのSCMS情報を要素として、
曲データベースに登録する
S257
曲データベース全体の
ハッシュ値を計算する
S258
エンド

FIG.27

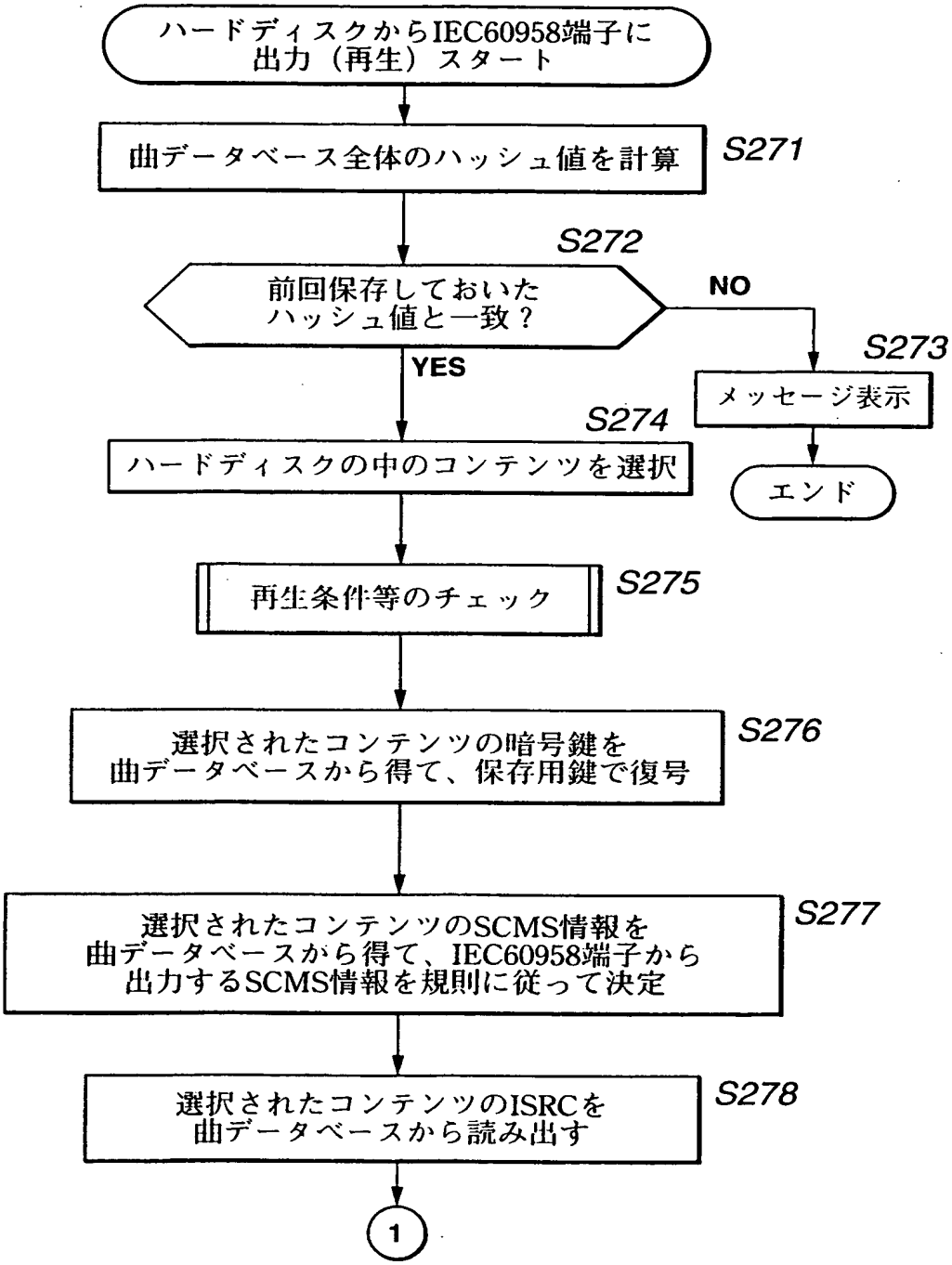

ハードディスクからIEC60958端子に
出力（再生）スタート
曲データベース全体のハッシュ値を計算
S271
S272
前回保存しておいた
ハッシュ値と一致？
NO
S273
メッセージ表示
エンド
YES
S274
ハードディスクの中のコンテンツを選択
再生条件等のチェック
S275
選択されたコンテンツの暗号鍵を
曲データベースから得て、保存用鍵で復号
S276
選択されたコンテンツのSCMS情報を
曲データベースから得て、IEC60958端子から
出力するSCMS情報を規則に従って決定
S277
選択されたコンテンツのISRCを
曲データベースから読み出す
S278
1

FIG.28

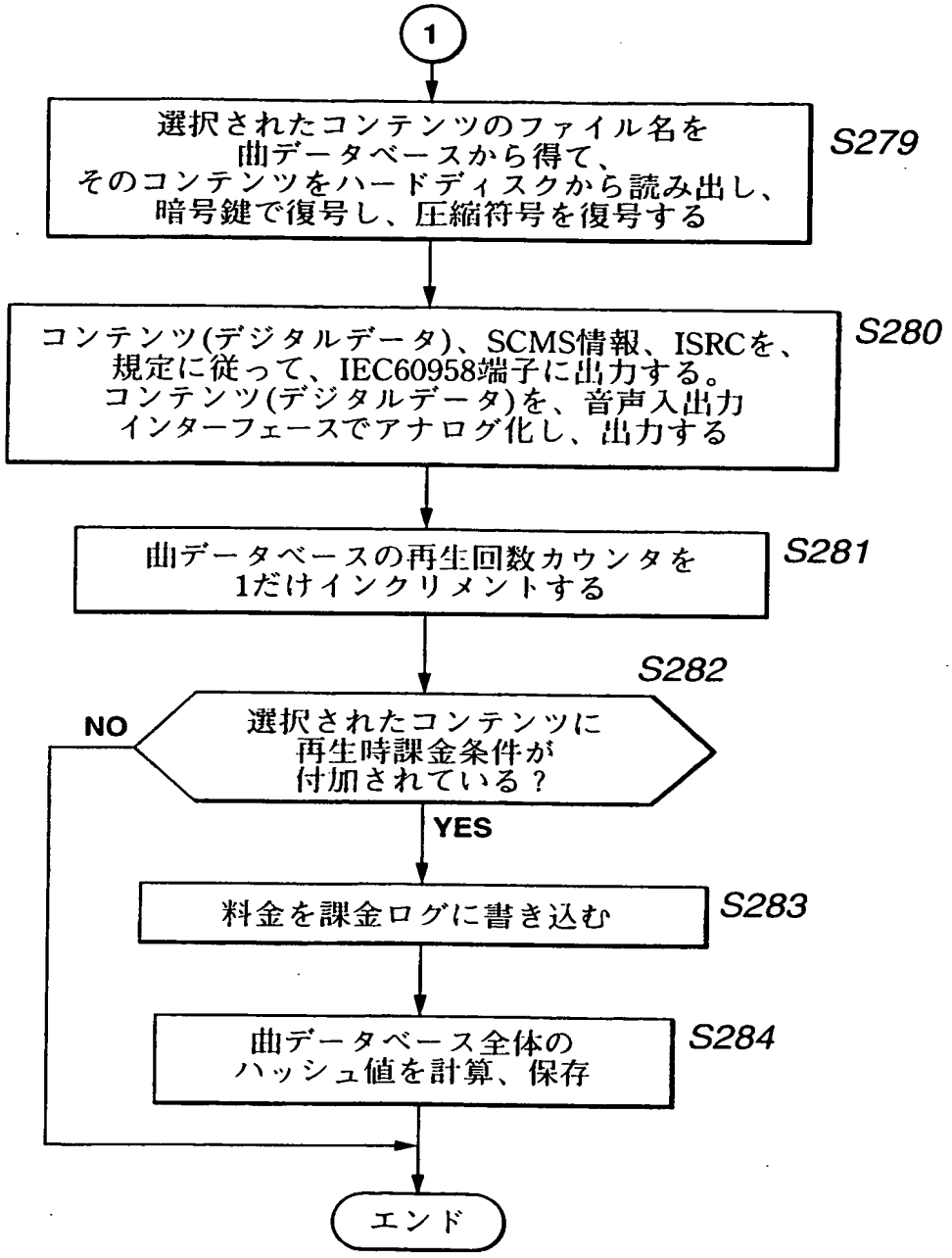

1
選択されたコンテンツのファイル名を
曲データベースから得て、
そのコンテンツをハードディスクから読み出し、
暗号鍵で復号し、圧縮符号を復号する
S279
コンテンツ(デジタルデータ)、SCMS情報、ISRCを、
規定に従って、IEC60958端子に出力する。
コンテンツ(デジタルデータ)を、音声入出力
インターフェースでアナログ化し、出力する
S280
曲データベースの再生回数カウンタを
1だけインクリメントする
S281
S282
NO
選択されたコンテンツに
再生時課金条件が
付加されている？
YES
料金を課金ログに書き込む
S283
曲データベース全体の
ハッシュ値を計算、保存
S284
エンド

FIG.29

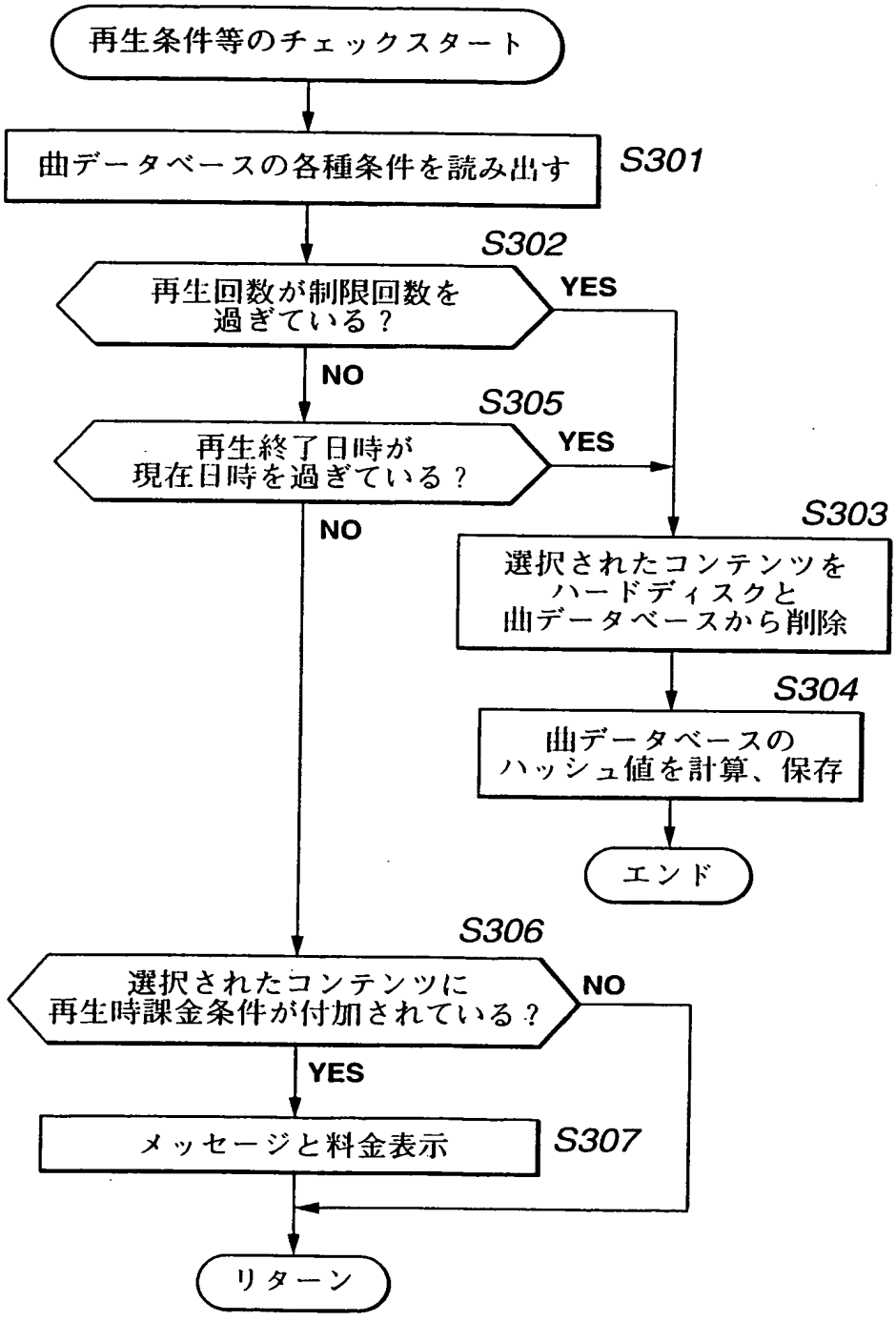

再生条件等のチェックスタート
曲データベースの各種条件を読み出す
S301
S302
再生回数が制限回数を過ぎている？
YES
NO
S305
再生終了日時が現在日時を過ぎている？
YES
NO
S303
選択されたコンテンツをハードディスクと曲データベースから削除
S304
曲データベースのハッシュ値を計算、保存
エンド
S306
選択されたコンテンツに再生時課金条件が付加されている？
NO
YES
メッセージと料金表示
S307
リターン

FIG.30

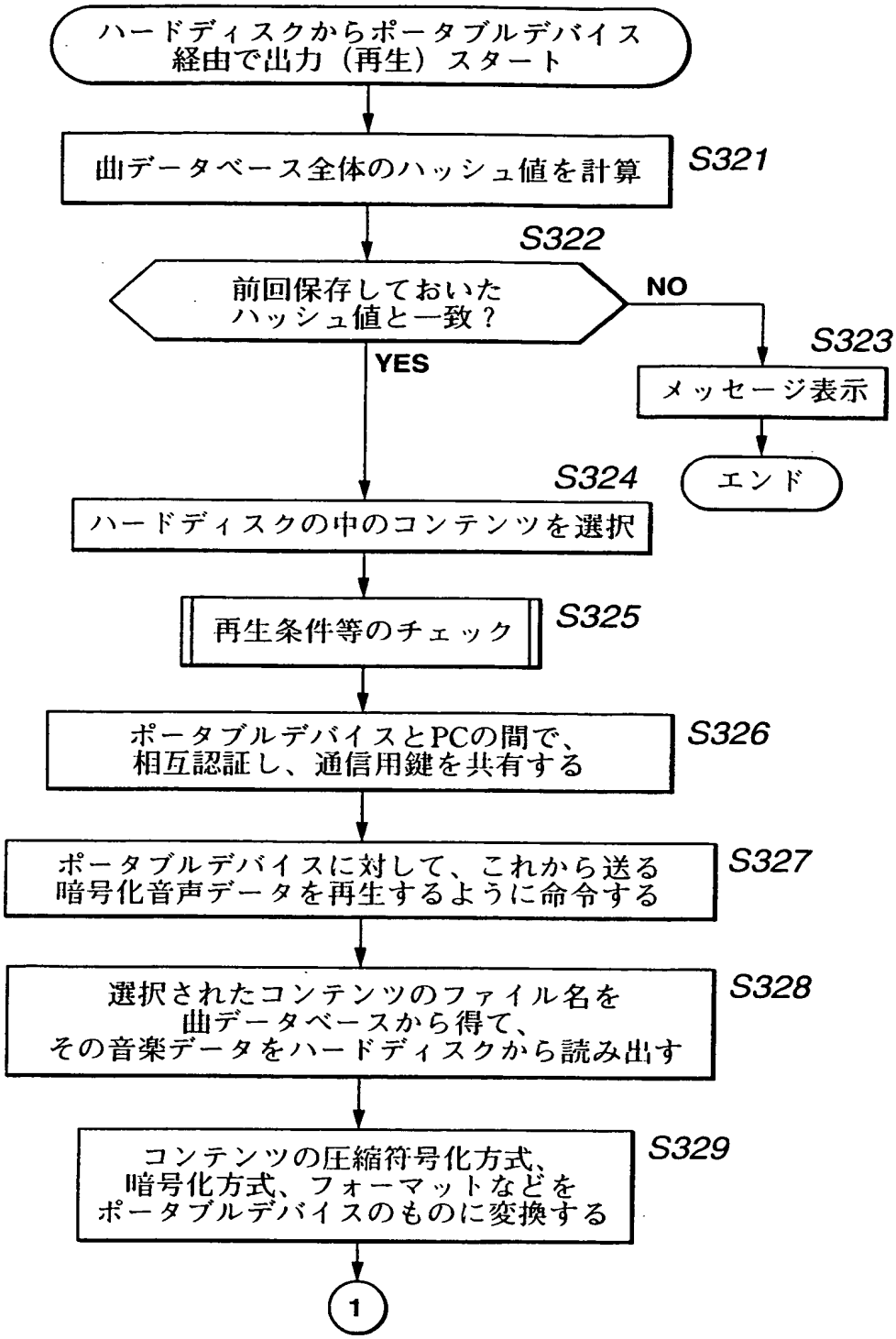

ハードディスクからポータブルデバイス
経由で出力（再生）スタート
曲データベース全体のハッシュ値を計算
S321
S322
前回保存しておいた
ハッシュ値と一致？
NO
YES
S323
メッセージ表示
エンド
S324
ハードディスクの中のコンテンツを選択
再生条件等のチェック
S325
ポータブルデバイスとPCの間で、
相互認証し、通信用鍵を共有する
S326
ポータブルデバイスに対して、これから送る
暗号化音声データを再生するように命令する
S327
選択されたコンテンツのファイル名を
曲データベースから得て、
その音楽データをハードディスクから読み出す
S328
コンテンツの圧縮符号化方式、
暗号化方式、フォーマットなどを
ポータブルデバイスのものに変換する
S329
1

FIG.31

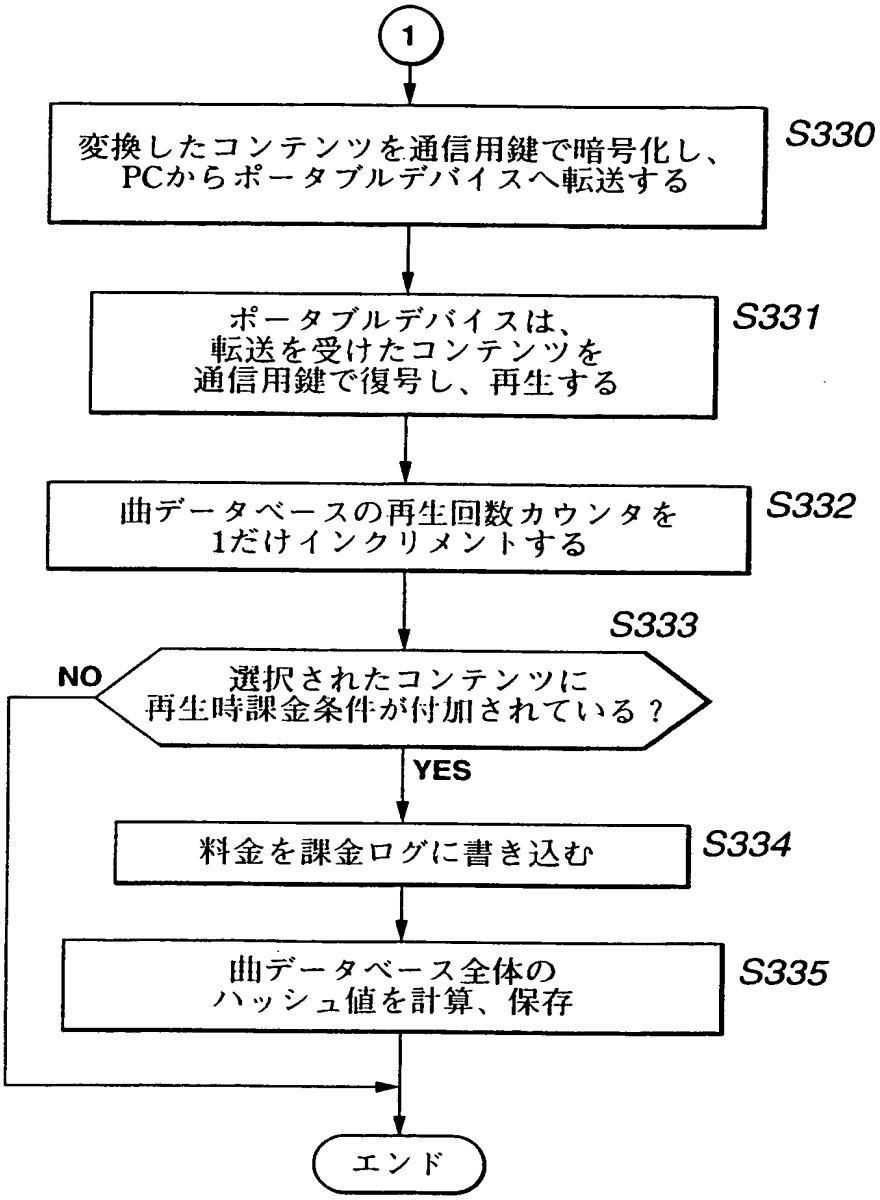

1
変換したコンテンツを通信用鍵で暗号化し、PCからポータブルデバイスへ転送する
S330
ポータブルデバイスは、転送を受けたコンテンツを通信用鍵で復号し、再生する
S331
曲データベースの再生回数カウンタを1だけインクリメントする
S332
S333
選択されたコンテンツに再生時課金条件が付加されている？
NO
YES
料金を課金ログに書き込む
S334
曲データベース全体のハッシュ値を計算、保存
S335
エンド

FIG.32

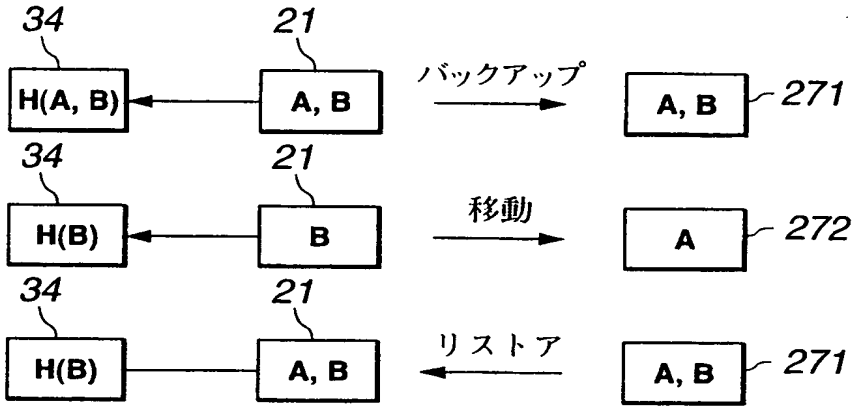

34
21
H(A, B)
A, B
バックアップ
A, B
271
34
21
H(B)
B
移動
A
272
34
21
H(B)
A, B
リストア
A, B
271

FIG.33

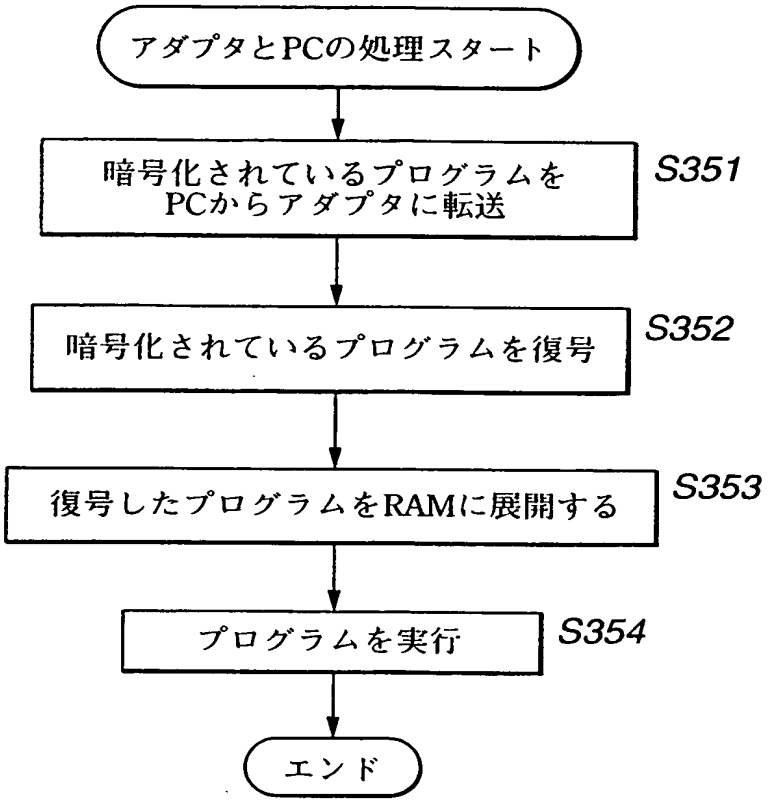

アダプタとPCの処理スタート
暗号化されているプログラムを
PCからアダプタに転送
S351
暗号化されているプログラムを復号
S352
復号したプログラムをRAMに展開する
S353
プログラムを実行
S354
エンド

FIG.34

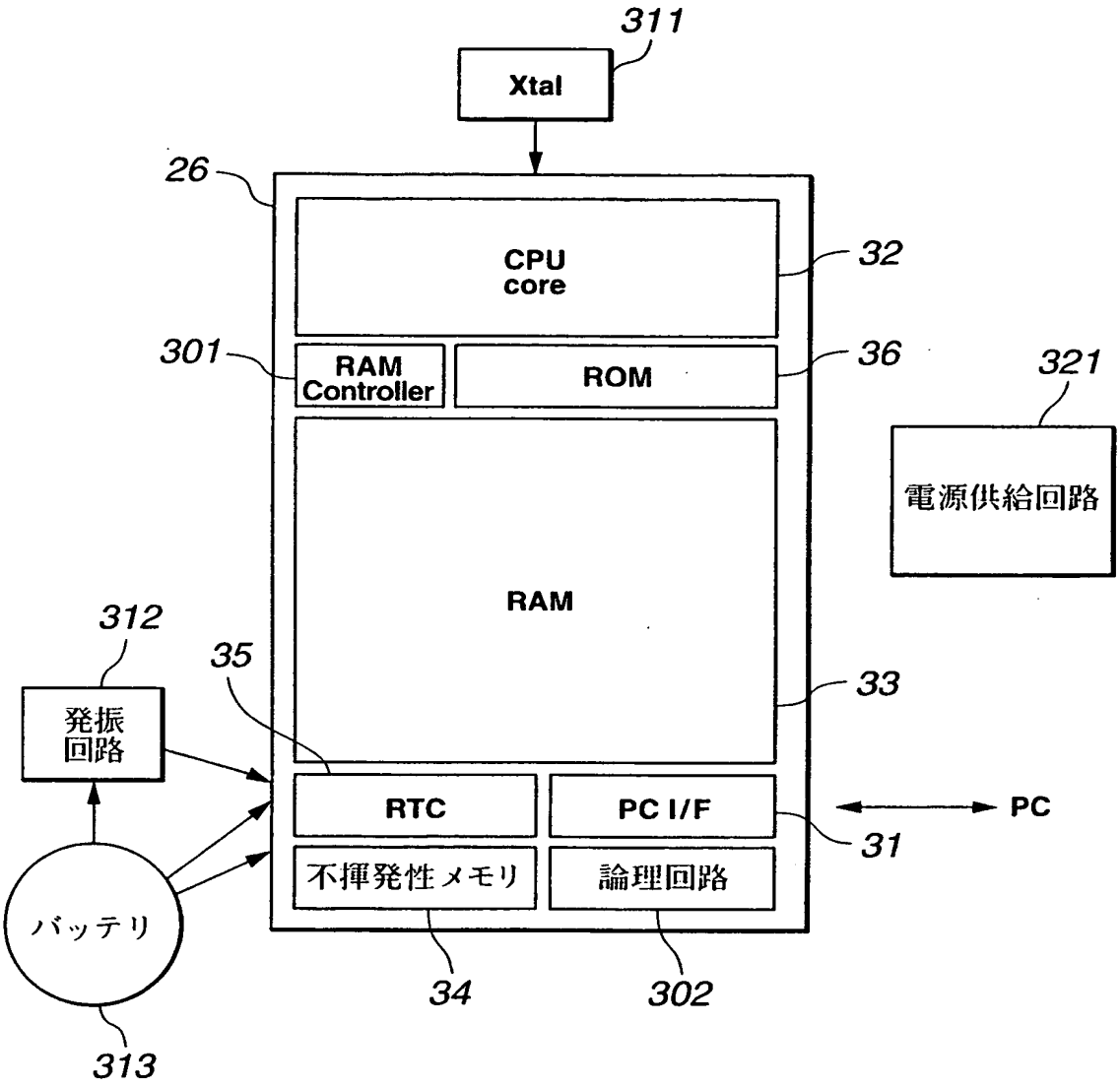

311
Xtal
26
CPU
core
32
301
RAM
Controller
ROM
36
321
電源供給回路
RAM
312
35
33
発振
回路
RTC
PC I/F
PC
31
不揮発性メモリ
論理回路
バッテリ
34
302
313

FIG.35

FIG.36A

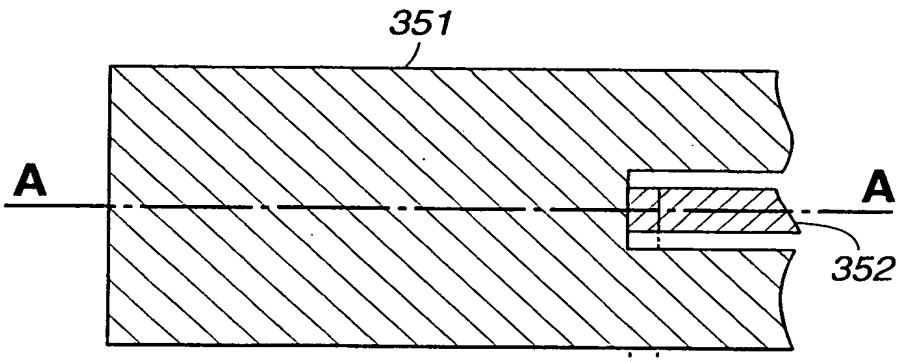
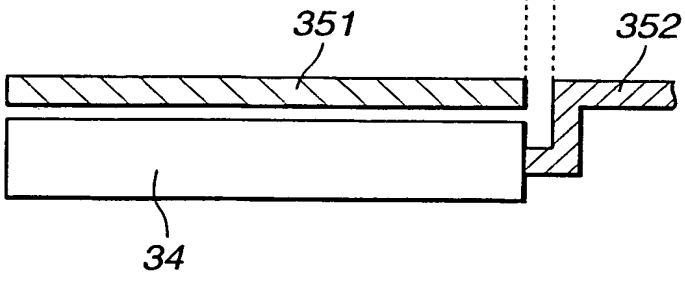


FIG.36B



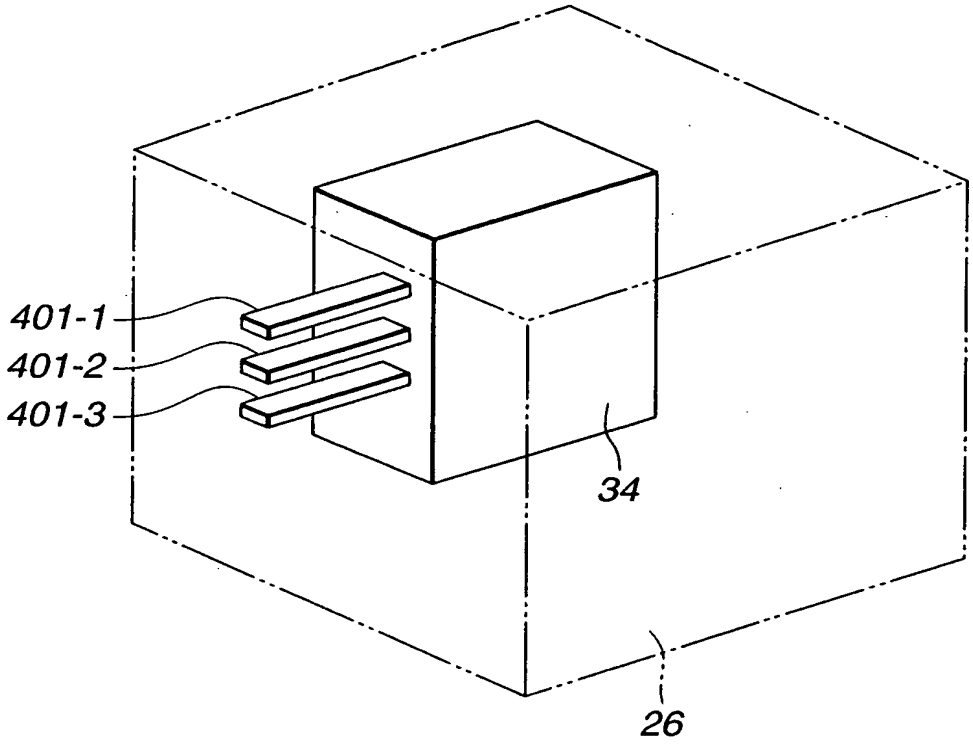


FIG.37

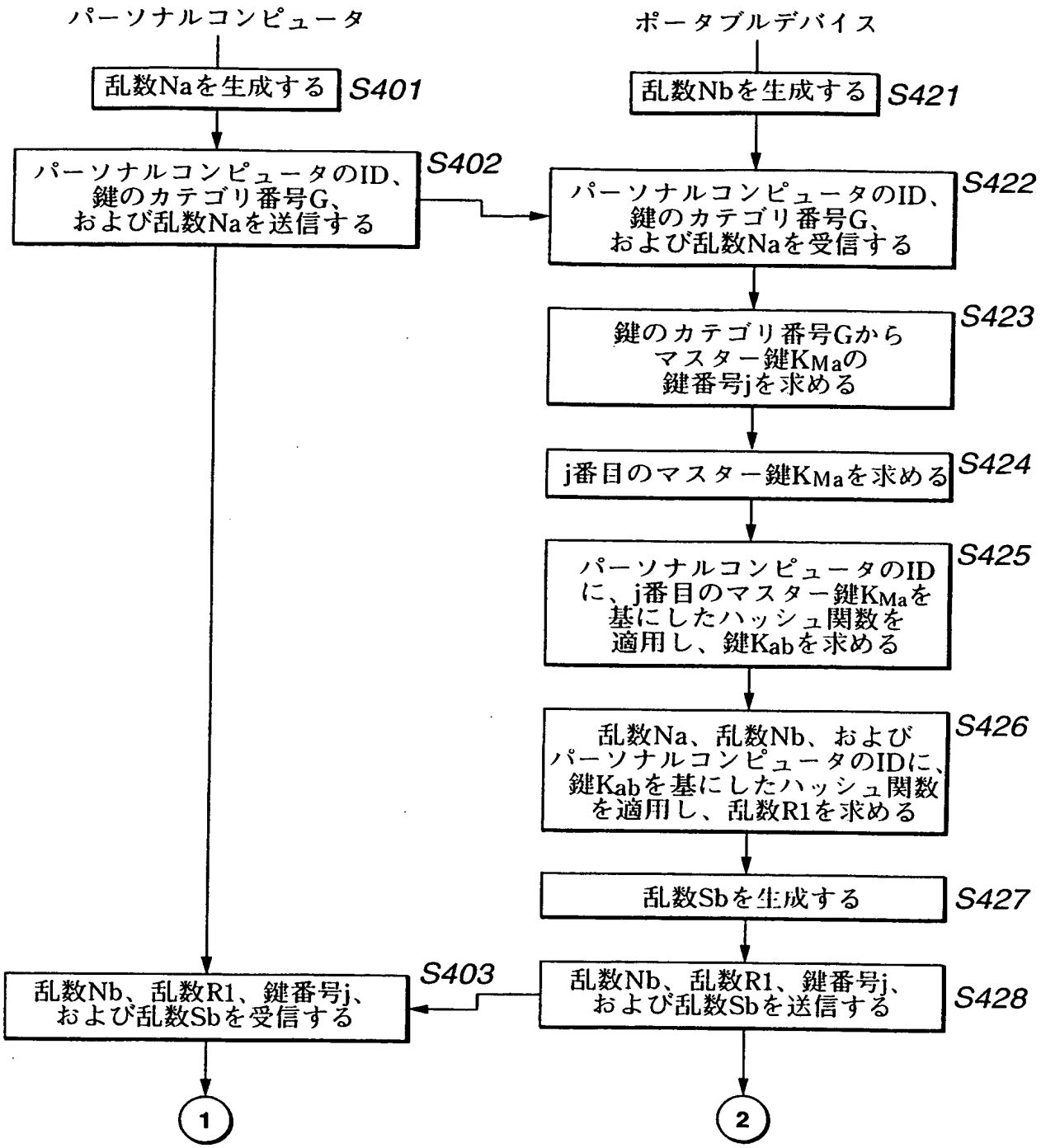

パーソナルコンピュータ
ポータブルデバイス
乱数Naを生成する
S401
乱数Nbを生成する
S421
パーソナルコンピュータのID、
鍵のカテゴリ番号G、
および乱数Naを送信する
S402
パーソナルコンピュータのID、
鍵のカテゴリ番号G、
および乱数Naを受信する
S422
鍵のカテゴリ番号Gから
マスター鍵KMaの
鍵番号jを求める
S423
j番目のマスター鍵KMaを求める
S424
パーソナルコンピュータのID
に、j番目のマスター鍵KMaを
基にしたハッシュ関数を
適用し、鍵Kabを求める
S425
乱数Na、乱数Nb、および
パーソナルコンピュータのIDに、
鍵Kabを基にしたハッシュ関数
を適用し、乱数R1を求める
S426
乱数Sbを生成する
S427
乱数Nb、乱数R1、鍵番号j、
および乱数Sbを受信する
S403
乱数Nb、乱数R1、鍵番号j、
および乱数Sbを送信する
S428
1
2

FIG.38

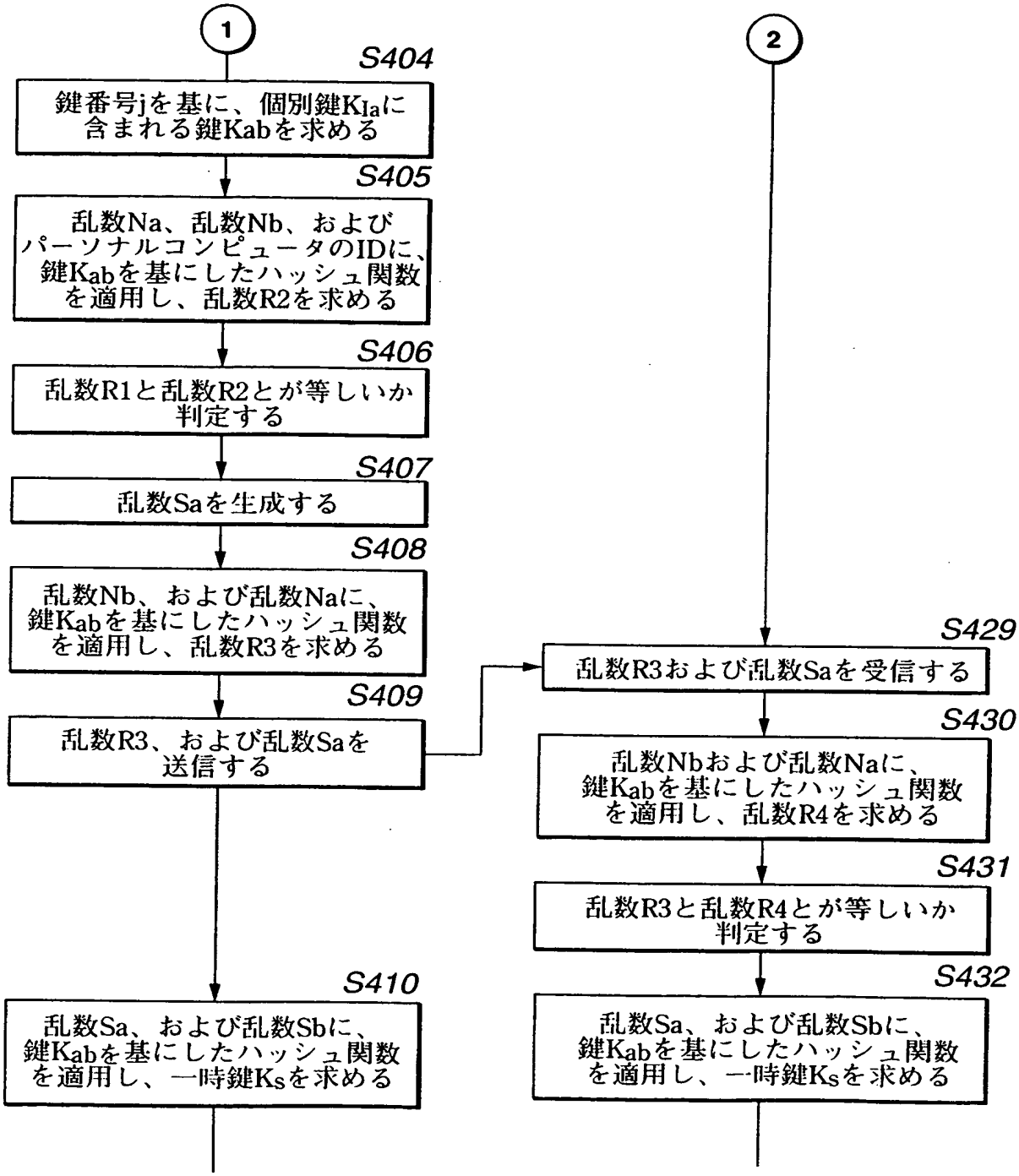

1
S404
鍵番号jを基に、個別鍵KIaに含まれる鍵Kabを求める
S405
乱数Na、乱数Nb、およびパーソナルコンピュータのIDに、鍵Kabを基にしたハッシュ関数を適用し、乱数R2を求める
S406
乱数R1と乱数R2とが等しいか判定する
S407
乱数Saを生成する
S408
乱数Nb、および乱数Naに、鍵Kabを基にしたハッシュ関数を適用し、乱数R3を求める
S409
乱数R3、および乱数Saを送信する
S410
乱数Sa、および乱数Sbに、鍵Kabを基にしたハッシュ関数を適用し、一時鍵Ksを求める
2
S429
乱数R3および乱数Saを受信する
S430
乱数Nbおよび乱数Naに、鍵Kabを基にしたハッシュ関数を適用し、乱数R4を求める
S431
乱数R3と乱数R4とが等しいか判定する
S432
乱数Sa、および乱数Sbに、鍵Kabを基にしたハッシュ関数を適用し、一時鍵Ksを求める

FIG.39

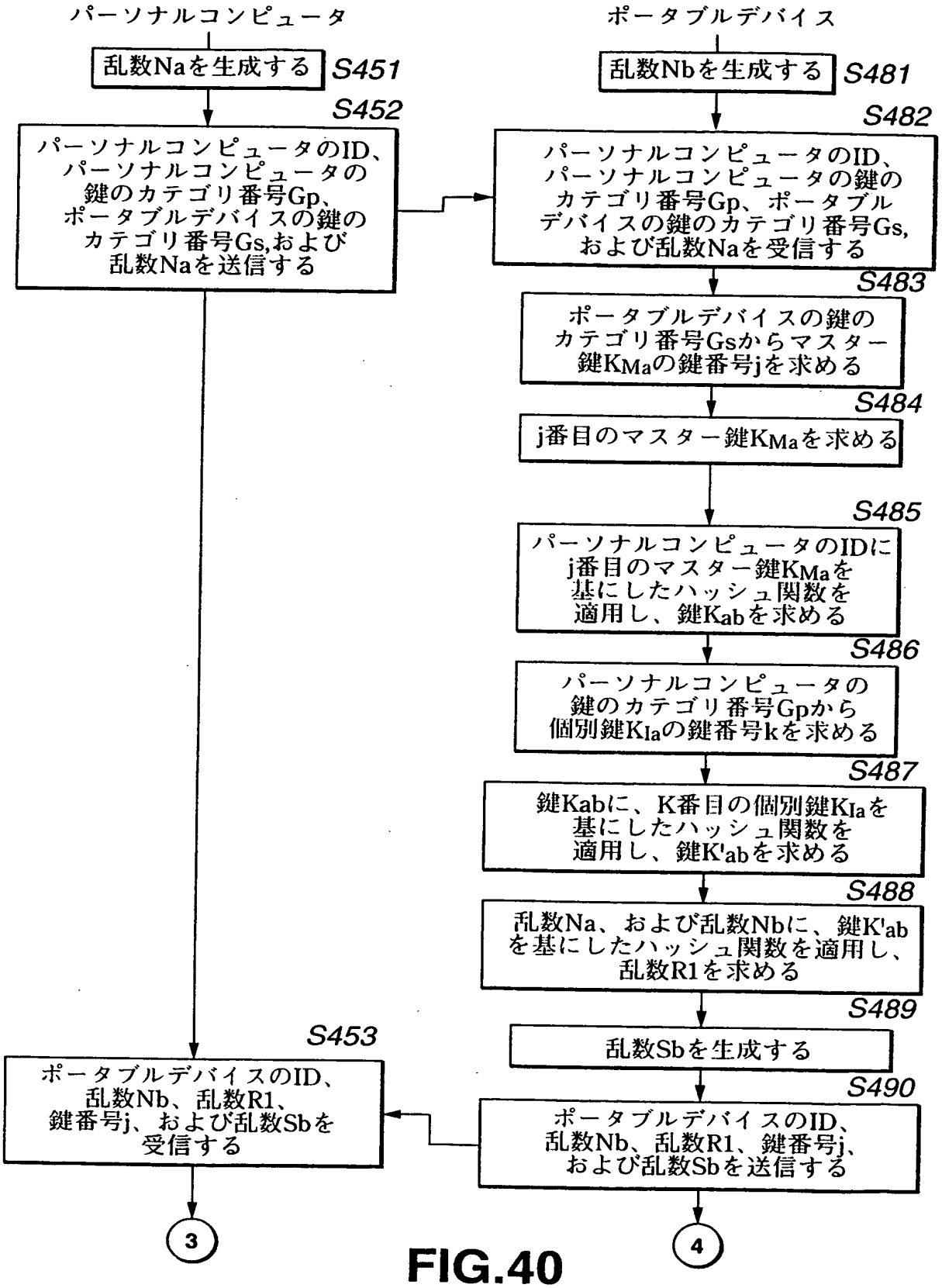

パーソナルコンピュータ
乱数Naを生成する
S451
S452
パーソナルコンピュータのID、パーソナルコンピュータの鍵のカテゴリ番号Gp、ポータブルデバイスの鍵のカテゴリ番号Gs,および乱数Naを送信する
S453
ポータブルデバイスのID、乱数Nb、乱数R1、鍵番号j、および乱数Sbを受信する
3
ポータブルデバイス
乱数Nbを生成する
S481
S482
パーソナルコンピュータのID、パーソナルコンピュータの鍵のカテゴリ番号Gp、ポータブルデバイスの鍵のカテゴリ番号Gs,および乱数Naを受信する
S483
ポータブルデバイスの鍵のカテゴリ番号Gsからマスター鍵KMaの鍵番号jを求める
S484
j番目のマスター鍵KMaを求める
S485
パーソナルコンピュータのIDにj番目のマスター鍵KMaを基にしたハッシュ関数を適用し、鍵Kabを求める
S486
パーソナルコンピュータの鍵のカテゴリ番号Gpから個別鍵Kiaの鍵番号kを求める
S487
鍵Kabに、K番目の個別鍵Kiaを基にしたハッシュ関数を適用し、鍵K'abを求める
S488
乱数Na、および乱数Nbに、鍵K'abを基にしたハッシュ関数を適用し、乱数R1を求める
S489
乱数Sbを生成する
S490
ポータブルデバイスのID、乱数Nb、乱数R1、鍵番号j、および乱数Sbを送信する
4

FIG.40

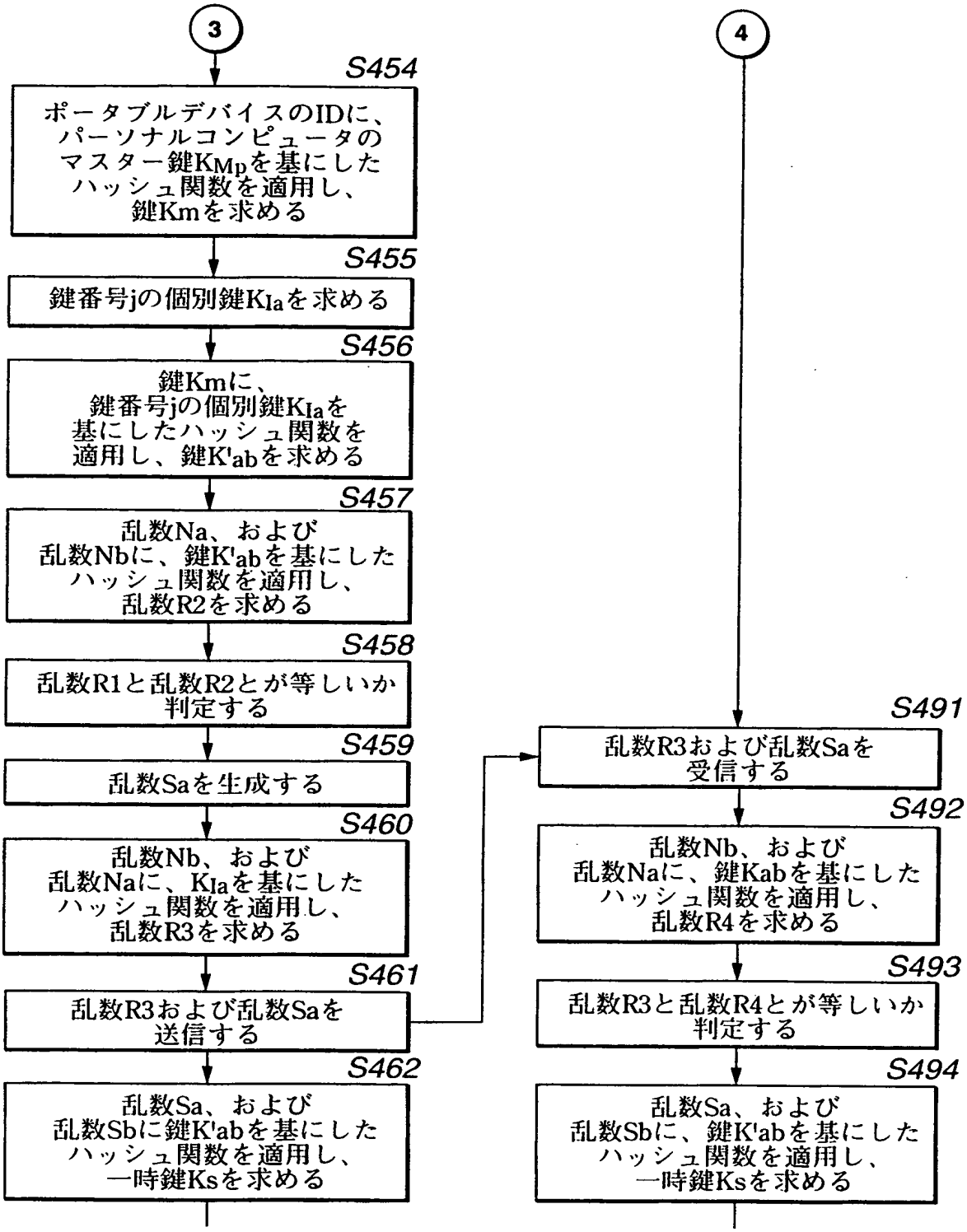

3
S454
ポータブルデバイスのIDに、パーソナルコンピュータのマスター鍵K_{Mp}を基にしたハッシュ関数を適用し、鍵Kmを求める
S455
鍵番号jの個別鍵K_{Ia}を求める
S456
鍵Kmに、鍵番号jの個別鍵K_{Ia}を基にしたハッシュ関数を適用し、鍵K'abを求める
S457
乱数Na、および乱数Nbに、鍵K'abを基にしたハッシュ関数を適用し、乱数R2を求める
S458
乱数R1と乱数R2とが等しいか判定する
S459
乱数Saを生成する
S460
乱数Nb、および乱数Naに、K_{Ia}を基にしたハッシュ関数を適用し、乱数R3を求める
S461
乱数R3および乱数Saを送信する
S462
乱数Sa、および乱数Sbに鍵K'abを基にしたハッシュ関数を適用し、一時鍵Ksを求める
4
S491
乱数R3および乱数Saを受信する
S492
乱数Nb、および乱数Naに、鍵Kabを基にしたハッシュ関数を適用し、乱数R4を求める
S493
乱数R3と乱数R4とが等しいか判定する
S494
乱数Sa、および乱数Sbに、鍵K'abを基にしたハッシュ関数を適用し、一時鍵Ksを求める

FIG.41

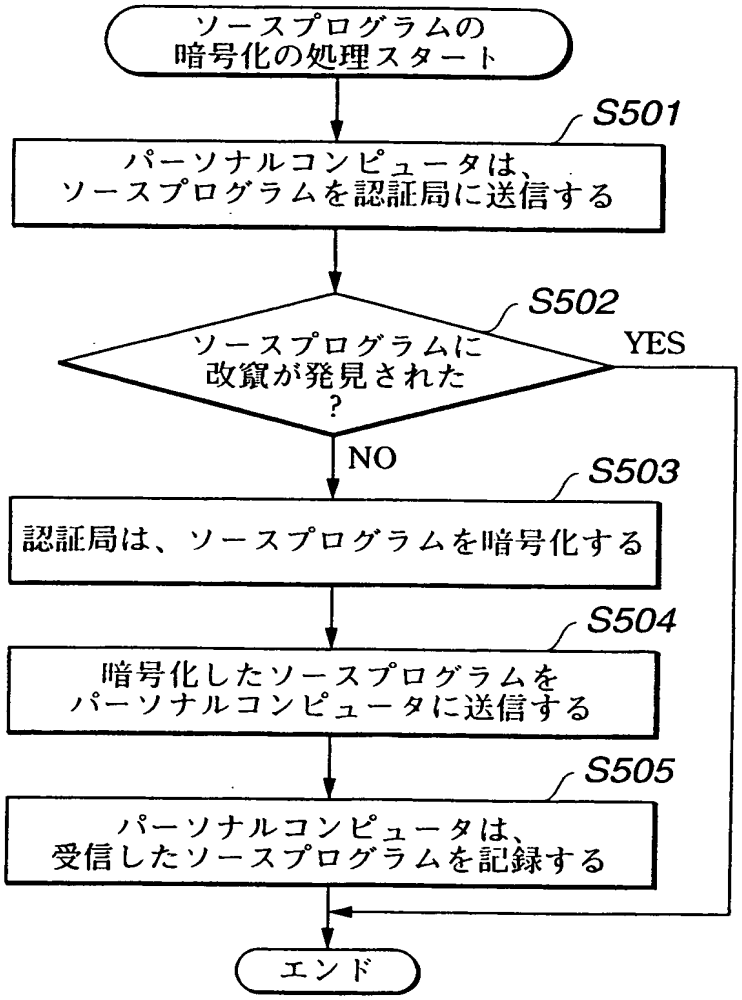

ソースプログラムの
暗号化の処理スタート
S501
パーソナルコンピュータは、
ソースプログラムを認証局に送信する
S502
ソースプログラムに
改竄が発見された
?
YES
NO
S503
認証局は、ソースプログラムを暗号化する
S504
暗号化したソースプログラムを
パーソナルコンピュータに送信する
S505
パーソナルコンピュータは、
受信したソースプログラムを記録する
エンド

FIG.42

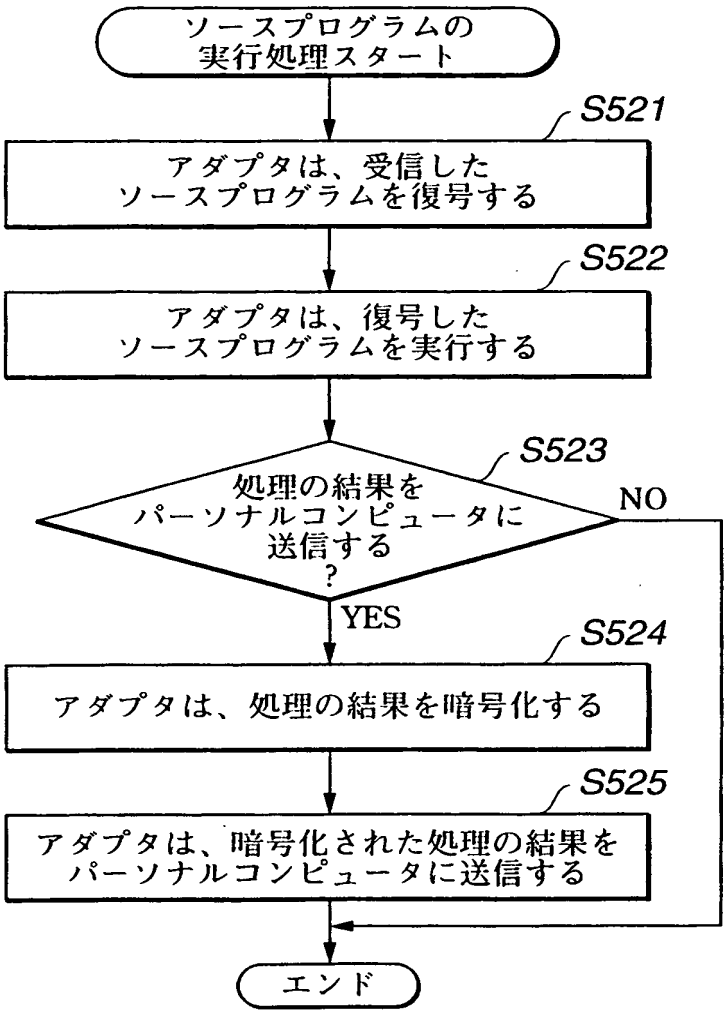

ソースプログラムの
実行処理スタート
S521
アダプタは、受信した
ソースプログラムを復号する
S522
アダプタは、復号した
ソースプログラムを実行する
S523
処理の結果を
パーソナルコンピュータに
送信する
?
NO
YES
S524
アダプタは、処理の結果を暗号化する
S525
アダプタは、暗号化された処理の結果を
パーソナルコンピュータに送信する
エンド

FIG.43

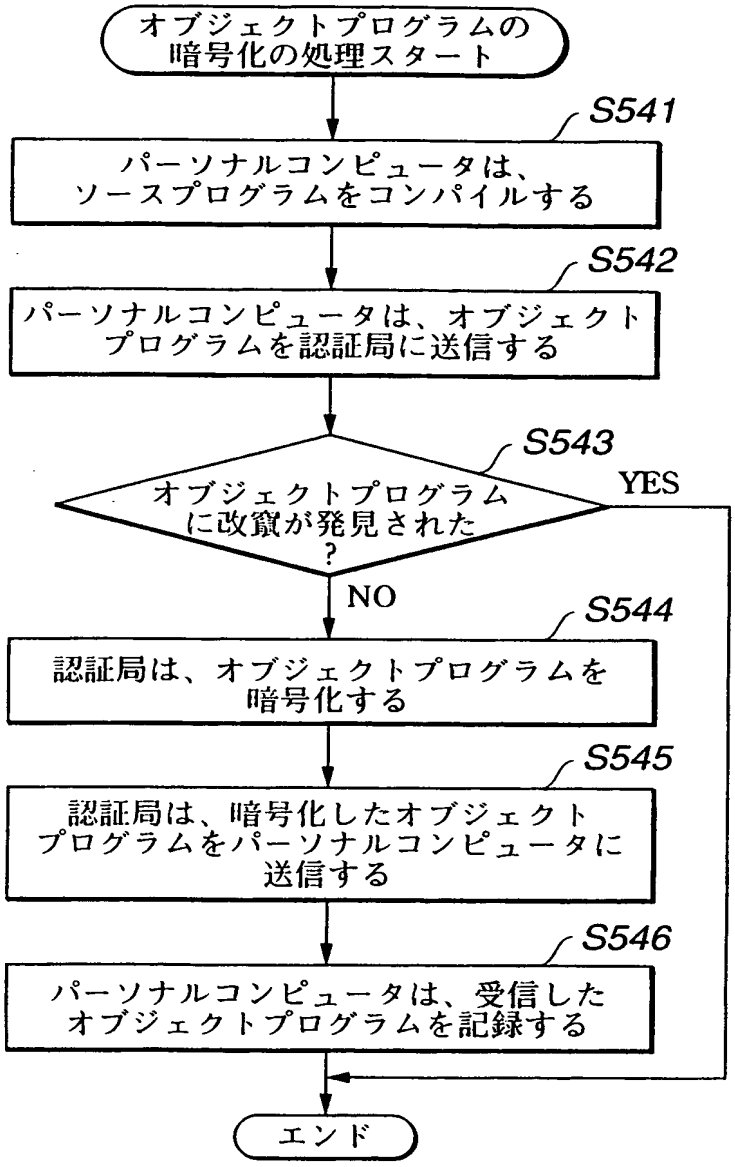

オブジェクトプログラムの
暗号化の処理スタート
S541
パーソナルコンピュータは、
ソースプログラムをコンパイルする
S542
パーソナルコンピュータは、オブジェクト
プログラムを認証局に送信する
S543
オブジェクトプログラム
に改竄が発見された
?
YES
NO
S544
認証局は、オブジェクトプログラムを
暗号化する
S545
認証局は、暗号化したオブジェクト
プログラムをパーソナルコンピュータに
送信する
S546
パーソナルコンピュータは、受信した
オブジェクトプログラムを記録する
エンド

FIG.44

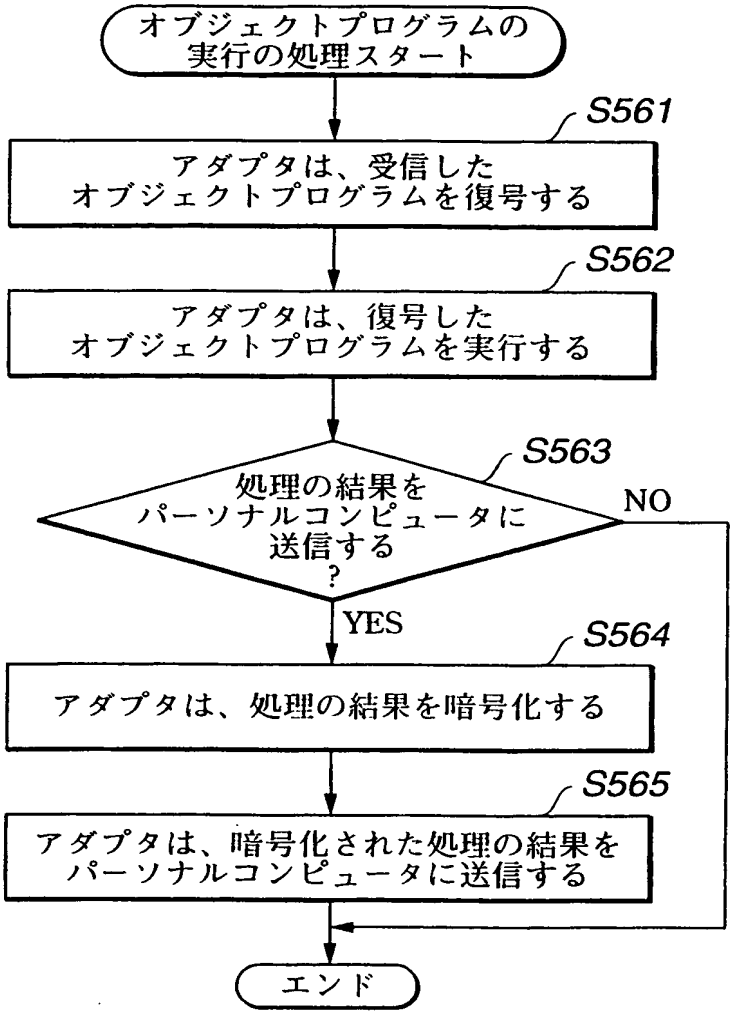

オブジェクトプログラムの
実行の処理スタート
S561
アダプタは、受信した
オブジェクトプログラムを復号する
S562
アダプタは、復号した
オブジェクトプログラムを実行する
S563
処理の結果を
パーソナルコンピュータに
送信する
?
NO
YES
S564
アダプタは、処理の結果を暗号化する
S565
アダプタは、暗号化された処理の結果を
パーソナルコンピュータに送信する
エンド

FIG.45

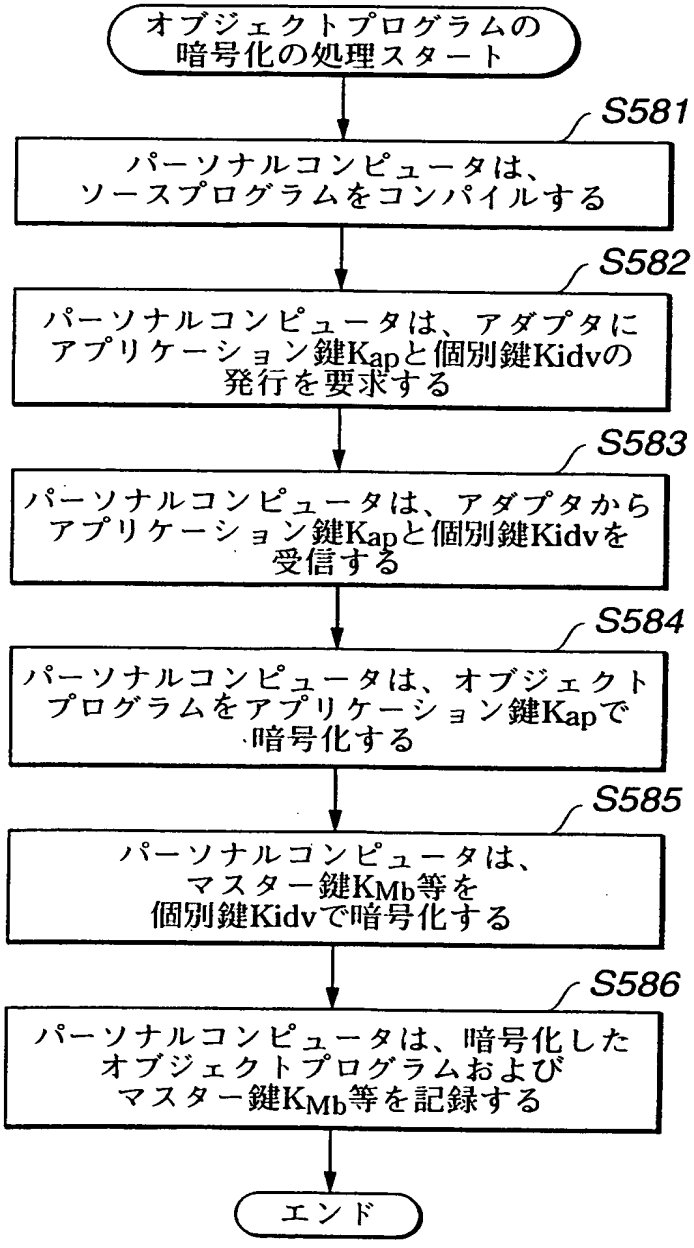

オブジェクトプログラムの暗号化の処理スタート
S581
パーソナルコンピュータは、ソースプログラムをコンパイルする
S582
パーソナルコンピュータは、アダプタにアプリケーション鍵Kapと個別鍵Kidvの発行を要求する
S583
パーソナルコンピュータは、アダプタからアプリケーション鍵Kapと個別鍵Kidvを受信する
S584
パーソナルコンピュータは、オブジェクトプログラムをアプリケーション鍵Kapで暗号化する
S585
パーソナルコンピュータは、マスター鍵KMb等を個別鍵Kidvで暗号化する
S586
パーソナルコンピュータは、暗号化したオブジェクトプログラムおよびマスター鍵KMb等を記録する
エンド

FIG.46

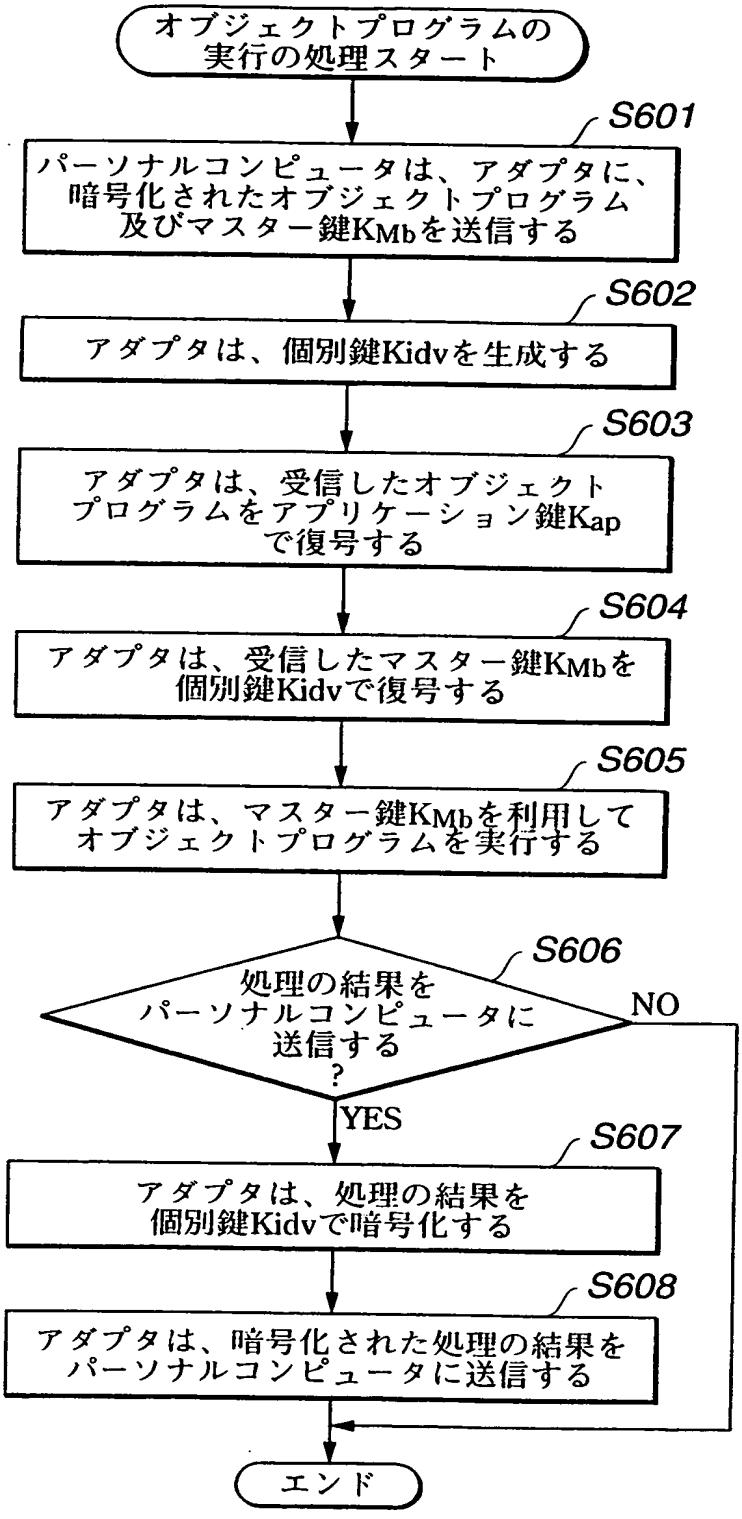

オブジェクトプログラムの実行の処理スタート
S601
パーソナルコンピュータは、アダプタに、暗号化されたオブジェクトプログラム及びマスター鍵KMbを送信する
S602
アダプタは、個別鍵Kidvを生成する
S603
アダプタは、受信したオブジェクトプログラムをアプリケーション鍵Kapで復号する
S604
アダプタは、受信したマスター鍵KMbを個別鍵Kidvで復号する
S605
アダプタは、マスター鍵KMbを利用してオブジェクトプログラムを実行する
S606
処理の結果をパーソナルコンピュータに送信する？
NO
YES
S607
アダプタは、処理の結果を個別鍵Kidvで暗号化する
S608
アダプタは、暗号化された処理の結果をパーソナルコンピュータに送信する
エンド

FIG.47

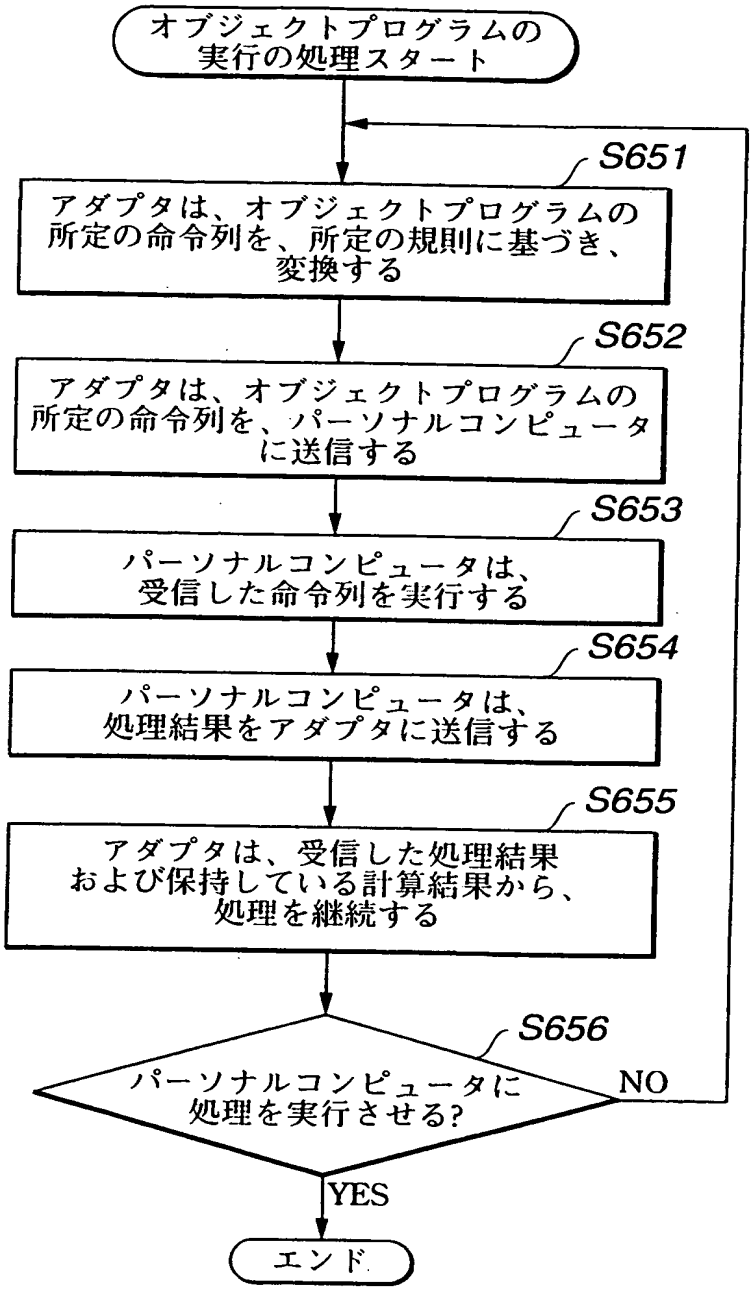

オブジェクトプログラムの
実行の処理スタート
S651
アダプタは、オブジェクトプログラムの
所定の命令列を、所定の規則に基づき、
変換する
S652
アダプタは、オブジェクトプログラムの
所定の命令列を、パーソナルコンピュータ
に送信する
S653
パーソナルコンピュータは、
受信した命令列を実行する
S654
パーソナルコンピュータは、
処理結果をアダプタに送信する
S655
アダプタは、受信した処理結果
および保持している計算結果から、
処理を継続する
S656
パーソナルコンピュータに
処理を実行させる?
NO
YES
エンド

FIG.48

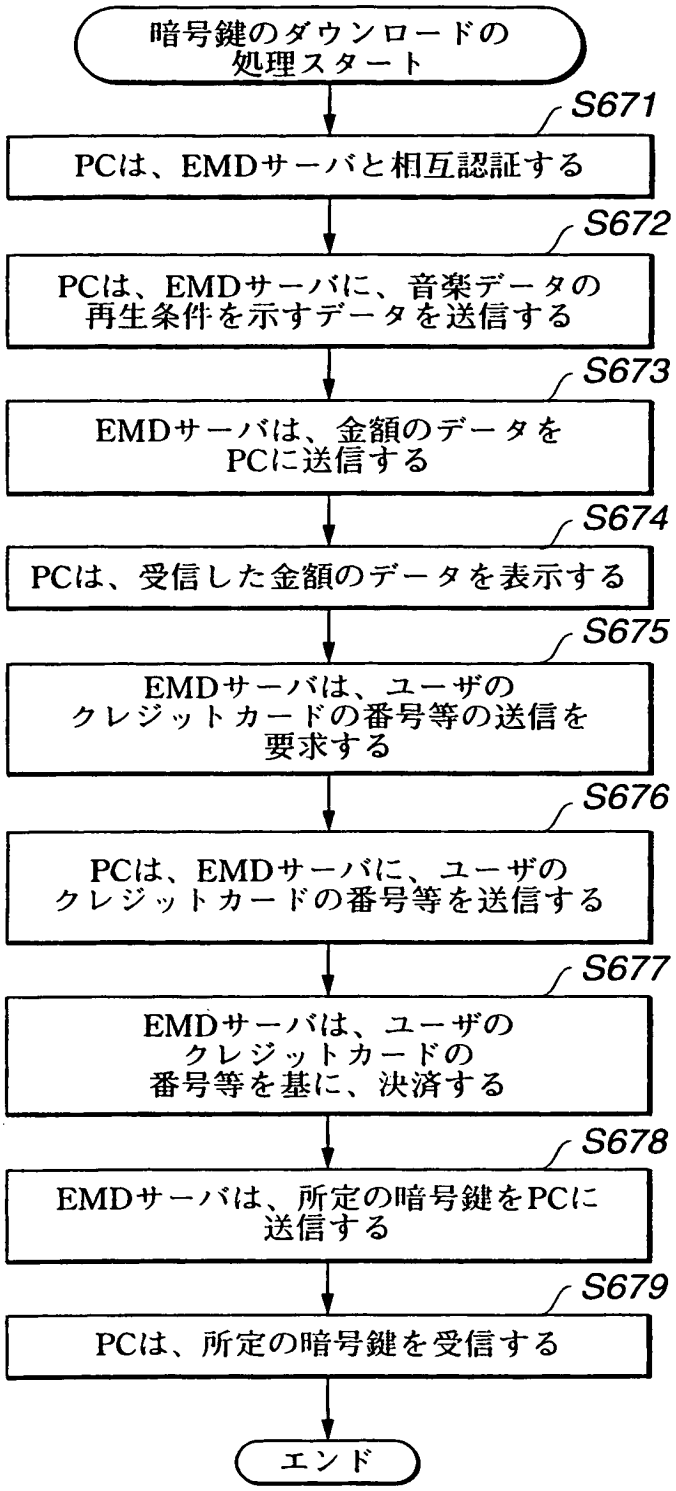

暗号鍵のダウンロードの処理スタート
S671
PCは、EMDサーバと相互認証する
S672
PCは、EMDサーバに、音楽データの再生条件を示すデータを送信する
S673
EMDサーバは、金額のデータをPCに送信する
S674
PCは、受信した金額のデータを表示する
S675
EMDサーバは、ユーザのクレジットカードの番号等の送信を要求する
S676
PCは、EMDサーバに、ユーザのクレジットカードの番号等を送信する
S677
EMDサーバは、ユーザのクレジットカードの番号等を基に、決済する
S678
EMDサーバは、所定の暗号鍵をPCに送信する
S679
PCは、所定の暗号鍵を受信する
エンド

FIG.49

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/02041

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F 1/00, 3/06, 3/08, 9/06, 9/445, 12/14, 13/00, 17/60
H04L 9/00~9/32
G09C 1/00~5/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DIALOG(INSPEC): OpenMG, MagicGate, MemoryStick
JICST(JOIST) : OpenMG, MagicGate, MemoryStick, Copyright, Contents Down Load

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Taro Yoshio, "Digital Chosakuken:Kogata Memory Card de Chosakuken wo mamoru", *Nikkei Electronics*, No.739, 22 March, 1999 (Tokyo), p.49-53	1-52
X Y	Taro Yoshio, "Ongaku Haishin matta nashi: Seibi Isogu Chosakuken Hogo Gijutsu", *Nikkei Electronics*, No.738, 08 March, 1999 (Tokyo), p.94-98	11-14 1-10,15-52
Y	EP, 875815, A2 (SONY CORPORATION), 04 November, 1998 (04.11.98), Full text; Figs. 1 to 16 & JP, 10-301772, A	1-5,15-52
Y	EP, 875814, A2 (SONY CORPORATION), 04 November, 1998 (04.11.98), Full text; Figs. 1 to 22 & JP, 10-301773, A	1-5,15-52
Y	EP, 862293, A2 (MATSUSHITA ELECTRIC INDUSTRIAL CO.LTD.), 02 September, 1998 (02.09.98), Full text; Figs. 1 to 9 & JP, 10-304333, A	6-8

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
21 June, 2000 (21.06.00)

Date of mailing of the international search report
04 July, 2000 (04.07.00)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/02041

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"DVD, Personal Computer ni noru Software Fukugou no Kagi wo nigiru Fusei Copy Boushi Gijutsu no Medo", *Nikkei Electronics*, No.696, 18 August, 1997 (Tokyo), p.110-119	9-10,15-52
Y	David Aucsmith, "Gyaku Kaiseki ya Kaihen kara Soft wo mamoru Tamper Resistant Software Gijutsu no Shousai", *Nikkei Electronics*, No.706, 05 January, 1998 (Tokyo), p.209-220	9-10,15-52
Y	EP, 874299, A2 (SONY CORPORATION), 28 October, 1998 (28.10.98), Full text; Figs. 1 to 32 & JP, 11-53264, A	9-10
Y	EP, 874300, A2 (SONY CORPORATION), 28 October, 1998 (28.10.98), Full text; Figs. 1 to 41 & JP, 11-53264, A	9-10
A	WO, 96/27155, A1 (INTERTRUST TECHNOLOGIES CORP.), 06 September, 1996 (06.09.96), Full text; Figs. 1 to 87 & JP, 10-512074, A	1-52

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/02041

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-5 relate to an information providing apparatus for receiving a program from a program information processing device over a network, encrypting the received program, and transmitting it to information processing device, to an information providing method, and to a program providing medium.

There is no special technical feature common to the inventions of claims 6-52 and those of claims 1-5.

For example, the inventions of claims 6-8 relate to an information processing apparatus for selecting a mutual authentication to be made from among mutual authentications between information processing devices and carrying out the mutual authentication, to an information processing method, and to a program providing medium.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０２０４１

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Ｉｎｔ　Ｃｌ⁷　Ｇ０６Ｆ９／０６

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Ｉｎｔ　Ｃｌ⁷　Ｇ０６Ｆ　1/00, 3/06, 3/08, 9/06, 9/445, 12/14, 13/00, 17/60
Ｈ０４Ｌ　９／００～９／３２
Ｇ０９Ｃ　１／００～５／００

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　１９２２－１９９６年
日本国公開実用新案公報　１９７１－２０００年
日本国登録実用新案公報　１９９４－２０００年
日本国実用新案登録公報　１９９６－２０００年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
DIALOG(INSPEC)：OpenMG, MagicGate, MemoryStick
JICST(JOIST)　：OpenMG, MagicGate, メモリースティック, 著作権, コンテンツ配信

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	日経エレクトロニクス, 第739号, 22. 3月. 1999(東京), 芳尾太郎, "ディジタル著作権：小型メモリ・カードで著作権を守る", p. 49-53	1-52
X Y	日経エレクトロニクス, 第738号, 08. 3月. 1999(東京), 芳尾太郎, "音楽配信待ったなし・整備急ぐ著作権保護技術", p. 94-98	11-14 1-10, 15-52
Y	EP, 875815, A2(SONY CORPORATION) 4. 11月. 1998(04. 11. 98) 全文, 第１～１６図 &JP, 10-301772, A	1-5, 15-52

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２１．０６．００	04.07.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	田川　泰宏	５Ｂ	４２３６
	電話番号　０３－３５８１－１１０１　内線　３５４５		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０２０４１

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	EP, 875814, A2 (SONY CORPORATION) 4. 11月. 1998 (04. 11. 98)　全文, 第１～２２図 &JP, 10-301773, A	1-5, 15-52
Y	EP, 862293, A2 (MATSUSHITA ELECTRIC INDUSTRIAL CO. LTD.) 2. 9月. 1998 (02. 09. 98)　全文, 第１～９図 &JP, 10-304333, A	6-8
Y	日経エレクトロニクス, 第696号, 18. 8月. 1997 (東京), "ＤＶＤ、パソコンに載る　ソフトウェア復号のカギを握る不正コピー防止技術のメド", p. 110-119	9-10, 15-52
Y	日経エレクトロニクス, 第706号, 05. 1月. 1998 (東京), David Aucsmith, "逆解析や改変からソフトを守る タンパ・レジスタント・ソフトウエア技術の詳細", p. 209-220	9-10, 15-52
Y	EP, 874299, A2 (SONY CORPORATION) 28. 10月. 1998 (28. 10. 98)　全文, 第１～３２図 &JP, 11-53264, A	9-10
Y	EP, 874300, A2 (SONY CORPORATION) 28. 10月. 1998 (28. 10. 98)　全文, 第１～４１図 &JP, 11-53264, A	9-10
A	WO, 96/27155, A1 (INTERTRUST TECHNOLOGIES CORP.) 6. 9月. 1996 (06. 09. 96)　全文, 第１～８７図 &JP, 10-512074, A	1-52

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０２０４１

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3. ☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１－５はネットワークを介してプログラムを情報処理装置からプログラムを受信し、受信したプログラムを暗号化して、前記情報処理装置に送信する構成を有する情報提供装置、情報提供方法およびプログラム提供媒体に関するものである。

一方、請求項６－５２については上記の構成とは共通の特別な技術的特徴はない。

たとえば、請求の範囲６－８は情報処理装置間の相互認証を行う際において、１以上の相互認証の手続きから、実行する相互認証の処理を選択し、実行する構成を有する情報処理装置、情報処理方法およびプログラム提供媒体に関するものである。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。